DOCUMENT RESUME

ED 099 980 EA 006 599

TITLE	Guidelines for Automatic Data Processing Physical Security and Risk Management. Federal Information Processing Standards Publication 31.
INSTITUTION	National Bureau of Standards (DOC), Washington, D.C.
REPORT NO	FIPS-PUB-31
PUB DATE	Jun 74
NOTE	99p.
AVAILABLE FROM	Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402 (SD Catalog C 13.52:31, $1.35)
EDRS PRICE	MF-$0.75 HC-$4.20 PLUS POSTAGE
DESCRIPTORS	*Computer Science; *Data Processing; Emergency Programs; *Facility Guidelines; Facility Requirements; Fire Protection; *Information Centers; Safety; *Security; Standards

ABSTRACT

These guidelines provide a handbook for use by federal organizations in structuring physical security and risk management programs for their automatic data processing facilities. This publication discusses security analysis, natural disasters, supporting utilities, system reliability, procedural measures and controls, off-site facilities, contingency plans, security awareness, and security audit. It contains statistics and information relevant to physical security of computer data and facilities and cites many applicable publications for a more exhaustive treatment of specific subjects. (Author)

ED 099 980

BEST COPY AVAILABLE

FIPS PUB 31

U.S. DEPARTMENT OF HEALTH
EDUCATION & WELFARE
NATIONAL INSTITUTE OF
EDUCATION
THIS DOCUMENT HAS BEEN REPRODUCED EXACTLY AS RECEIVED FROM THE PERSON OR ORGANIZATION ORIGINATING IT. POINTS OF VIEW OR OPINIONS STATED DO NOT NECESSARILY REPRESENT OFFICIAL NATIONAL INSTITUTE OF EDUCATION POSITION OR POLICY

FEDERAL INFORMATION
PROCESSING STANDARDS PUBLICATION

1974 JUNE

U.S. DEPARTMENT OF COMMERCE / National Bureau of Standards

ED 099 980

Guidelines

FOR AUTOMATIC DATA PROCESSING PHYSICAL SECURITY AND RISK MANAGEMENT

CATEGORY: ADP OPERATIONS
SUBCATEGORY: COMPUTER SECURITY

EA 006 599

BEST COPY AVAILABLE

Foreword

The Federal Information Processing Standards Publication Series of the National Bureau of Standards is the official publication relating to standards adopted and promulgated under the provisions of Public Law 89-306 (Brooks Bill) and under Part 6 of Title 15, Code of Federal Regulations. These legislative and executive mandates have given the Secretary of Commerce important responsibilities for improving the utilization and management of computers and automatic data processing systems in the Federal Government. To carry out the Secretary's responsibilities, the NBS, through its Institute for Computer Sciences and Technology, provides leadership, technical guidance, and coordination of government efforts in the development of guidelines and standards in these areas.

The subject areas of personal privacy, data confidentiality and computer security are of the greatest national interest. The Secretary of Commerce has identified the efforts required to provide solutions to technical problems encountered in these areas as personal objectives in the Department's overall program.

Data confidentiality and computer security are dependent upon the application of a balanced set of managerial and technological safeguards. Within the context of a total security program, the NBS is pleased to make these Guidelines for ADP Physical Security and Risk Management available for use by Federal agencies.

RUTH M. DAVIS, *Director*
Institute for Computer Sciences
and Technology

Abstract

This publication provides guidelines to be used by Federal organizations in structuring physical security programs for their ADP facilities. It treats security analysis, natural disasters, supporting utilities, system reliability, procedural measures and controls, off-site facilities, contingency plans, security awareness and security audit. It contains statistics and information relevant to physical security of computer data and facilities and references many applicable publications for a more exhaustive treatment of specific subjects.

Keywords: ADP security; computer reliability; contingency plans; Federal Information Processing Standard; fire safety. natural disasters; physical security; risk analysis; security audit; security awareness; supporting utilities.

Nat. Bur. Stand. (U.S.), Fed. Info. Process. Stand. Publ. (FIPS PUB) 31, 92 pages,
(1974) CODEN: FIPPAT

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402. (Order by SD Catalog C 13.52:31) GPO, price $1.35. Subscription service also available for all new FIPS publications and supplements for an indefinite period.

Federal Information Processing Standards Publication 31

1974 June

ANNOUNCING THE

GUIDELINES FOR AUTOMATIC DATA PROCESSING PHYSICAL SECURITY AND RISK MANAGEMENT

Federal Information Processing Standards Publications are issued by the National Bureau of Standards pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973), and Part 6 of Title 15 CFR (Code of Federal Regulations).

Name of Standard. Guidelines for Automatic Data Processing Physical Security and Risk Management.

Category of Standard. ADP Operations, Computer Security.

Explanation: These guidelines provide a handbook for use by Federal organizations in structuring physical security and risk management programs for their ADP facilities. This publication discusses security analysis, natural disasters, supporting utilities, system reliability, procedural measures and controls, off-site facilities, contingency plans, security awareness, and security audit. It contains statistics and information relevant to physical security of computer data and facilities and references many applicable publications for a more exhaustive treatment of specific subjects.

Approving Authority. Department of Commerce, National Bureau of Standards (Institute for Computer Sciences and Technology).

Maintenance Agency. Department of Commerce National Bureau of Standards (Institute for Computer Sciences and Technology).

Cross Index. None.

Applicability. These Guidelines are intended as basic reference document and a checklist for general use throughout the Federal Government to evaluate computer security and plan physical security programs in ADP systems.

Implementation. As new ADP systems are developed and current systems improved, these Guidelines should be utilized. Each organization should analyze its requirements for protection of data and processing facilities and implement the recommendations found in these Guidelines commensurate to its calculated risk. Depending upon differing operational requirements, facilities will require various levels of security protection. These Guidelines should assist the installation of managers in making, and justifying essential security decisions.

Specifications. Federal Information Processing Standard 31 (FIPS 31), Guidelines for Automatic Data Processing Physical Security and Risk Management, (affixed).

Qualifications. The statistics and recommendations provided in these Guidelines are based upon data and information supplied from many sources within the government and private sectors and reflect current practice and technologies. As new knowledge, techniques, and equipments become available in the future, these Guidelines will need to be modified accordingly. As experiences are gained through use and application of these Guidelines, a basis for security standards may be established. In this regard, comments and critiques concerning applications experience will be welcomed. These should be addressed to the Associate Director for ADP Standards, Institute for Computer Sciences and Technology, National Bureau of Standards, Washington, D.C. 20234.

Where to Obtain Copies of the Standard.

a. Copies of this publication are available from the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402 (SD Catalog Number C13.52:31). There is a 25 percent discount on quantities of 100 or more. When ordering, specify document number, title, and SD Catalog Number. Payment may be made by check, money order, coupons, or deposit account.

b. Microfiche of this publication is available from the National Technical Information Service, U.S. Department of Commerce, Springfield, Virginia 22151. When ordering refer to Report Number NBS-FIPS-PUB-31 and title. Payment may be made by check, money order, coupons, or deposit account.

Federal Information
Processing Standards Publication 31

1974 June

Specifications for

GUIDELINES FOR AUTOMATIC DATA PROCESSING PHYSICAL SECURITY AND RISK MANAGEMENT

Contents

Page

Action Summary 5

1. ADP Security Analysis 8
  - 1.0 Introduction 8
  - 1.1 Scope 8
  - 1.2 Threat to ADP Operations 9
  - 1.3 Risk Analysis 9
    - 1.3.1 Loss Potential Estimate 9
    - 1.3.2 Threat Analysis 11
    - 1.3.3 Annual Loss Expectancy 11
    - 1.3.4 Selecting Remedial Measures 13
  - 1.4 Implementing the Security Program 14
  - 1.5 Supporting Documents 15

2. Anticipating Natural Disasters 15
  - 2.0 Introduction 15
  - 2.1 Fire Safety 15
    - 2.1.1 ADP Facility Fire Exposure 16
    - 2.1.2 Fire Detection 17
    - 2.1.3 Fire Extinguishment 18
    - 2.1.4 Fire Fighting 20
  - 2.2 Flood 21
  - 2.3 Earthquake 23
  - 2.4 Windstorms 23

3. Supporting Utilities 27
  - 3.0 Introduction 27
  - 3.1 Electric Power 27
  - 3.2 Air Conditioning 34
  - 3.3 Communications Circuit 39
  - 3.4 Other Supporting Utilities 42

4. Computer System Reliability 42
  - 4.0 Introduction 42
  - 4.1 Computer System Reliability 42
  - 4.2 Management of Hardware Maintenance 43
  - 4.3 Reliability Considerations for New Systems 44

5. Physical Protection of ADP Facilities 45
  - 5.0 Introduction 45
  - 5.1 Determining Protection Requirements 45
    - 5.1.1 Instructions for the Facility Physical Security Survey 46
  - 5.2 Boundary Protection 47
    - 5.2.1 Emanations 48
  - 5.3 Entrance Door Controls 48
  - 5.4 Perimeter Intrusion Controls 49
  - 5.5 Critical Area Controls 50
  - 5.6 Guard Force Operations 53
  - 5.7 Integrating Physical Security Measures 54

6. Internal Controls 54
  - 6.0 Introduction 54
  - 6.1 Personnel Controls 55
    - 6.1.1 Personnel Selection 55
    - 6.1.2 Training 55
    - 6.1.3 Supervision 55
  - 6.2 Organizing for Internal Control 56
  - 6.3 Data Controls 59
  - 6.4 Data Retention and Back-Up 59
    - 6.4.1 Short Term Back-Up 59
    - 6.4.2 Long Term Back-Up 59
  - 6.5 Programming Controls 60
    - 6.5.1 Program Design 60
    - 6.5.2 Program Installation 60
    - 6.5.3 Documentation of Controls 62

7. Security of Off-Site ADP Facilities 62
  - 7.0 Introduction 62
  - 7.1 Analysis of Security Requirements 63
  - 7.2 On-Site Security 63
  - 7.3 In-Transit Security 64
  - 7.4 Off-Site Security 64

8. Contingency Planning 65
  - 8.0 Introduction 65
  - 8.1 Preparation of Contingency Plans 65
  - 8.2 Emergency Response Planning 68
  - 8.3 Back-Up Operations Planning 69
  - 8.4 Recovery Planning 71
  - 8.5 Testing Contingency Plans 73

9. Security Awareness and Communications 73
  - 9.0 Introduction 73

Page
9.1 Senior Management 74
9.2 Communicating the Security Program 74
9.2.1 Target Audience for the ADP Security Plan 74
9.2.2 Content of Communication Plan 74
9.2.3 Method of Communication 74
9.3 Summary 75

10. Internal Audit of Physical Security 75

10.0 Introduction 75
10.1 Audit Preparation 76
10.2 The Audit Plan 76
10.3 Conducting the Audit 81
10.4 Follow-up 82

Appendices

A. **Glossary** 83

B. Bibliography 84

C. Sample Table of Contents of Programming Procedures 86

Index 91

Acknowledgments

The Institute for Computer Sciences and Technology acknowledges Robert V. Jacobson, Vice President of SENTOR Security Group, Inc., as the principal author of this publication, and Dr. William F. Brown of Ball State University and Peter S. Browne of General Electric Information Systems as contributing authors. The work was done under contract to the Systems and Software Division of the Institute.

The Institute wishes to thank the Office of Federal Protective Services Management, General Services Administration and the Federal Fire Council, as well as the Safety and Fire Protection Section of NBS and the NBS Fire Protection Service for their scrutiny of pertinent chapters and suggestions for modification.

The Institute is grateful to Alfred M. Pfaff, Research Associate sponsored by the IBM Corporation, for reviewing the entire document, especially the figures, and effecting much contextual revision, including the above mentioned modifications.

The manuscript was edited for publication by Susan K. Reed, Systems and Software Division.

Action Summary

The essential recommendations from this publication are summarized here to show the scope of these guidelines and to provide a quick overview of action items in establishing, implementing and maintaining a physical security program in an ADP facility.

I. Organize The ADP Physical Security Program

Assign responsibility for ADP Physical Security and establish a task force to prepare a plan for the ADP security program.

Perform a preliminary risk analysis to identify major problem areas and select interim security measures as needed to correct major problem areas.

II. Conduct A Risk Analysis

Estimate potential losses to the ADP facility and its users from (1) physical destruction or theft of physical assets; (2) loss or destruction of data and program files; (3) theft of information; (4) theft of indirect assets; and (5) delay or prevention of computer processing.

Estimate the probability of occurrence for potential threats and their effect on the ADP facility in terms of the five classes of loss potential.
Combine the estimates of loss potential and threat probability to develop an annual loss expectancy.

Select the array of remedial measures which effects the greatest reduction in the annual loss expectancy at the least total cost. Remedial measures will include: (1) changes in the environment to reduce exposure; (2) measures to reduce the effect of a threat; (3) improved control procedures; (4) early detection; and (5) contingency plans.

III. Determine Local Natural Disaster Probabilities

Evaluate the fire safety of the ADP facility (building location, construction, occupancy and housekeeping) and provide required fire detection and extinguishment, and possibly a trained fire fighting brigade.

Evaluate the exposure to flooding from internal and external sources. Where needed, provide flood protection for the building relocate ADP hardware, reroute plumbing lines and provide water damage/flood-control equipment (pumps, tarpaulins, etc.)
Evaluate resistance of the building to wind and water damage if exposed to hurricanes, tornadoes or other high winds.

IV. Initiate A Security Program

Prepare a plan and a schedule for implementing selected remedial measures. Prepare and maintain a policy and plans handbook to include: (1) an ADP physical security policy statement; (2) mandatory security procedures; (3) security guidelines for system design, programming, testing, and maintenance; (4) contingency plans; (5) security indoctrination materials; and (6) a security audit program.

V. Protect Supporting Utilities

Estimate the number and duration of electric power transients, undervoltage conditions and power interruptions and their annual loss expectancy. Install appropriate protective equipment such as: voltage regulating transformers, dual power feeders, uninterruptible power supplies, on-site power generators and ADP power isolation circuits.

Estimate annual loss expectancy from air conditioning failures considering required operation schedules, annual profiles of local temperature and humidity, and an estimated number and duration of air conditioning failures. Where necessary, increase reliability with redundant equipment, provide for emergency use of outside air and augment maintenance capability to decrease mean time to repair.

Estimate the annual loss expectancy from teleprocessing circuit failures. Where cost is justified, increase reliability with redundant communications circuits and augment repair facilities to decrease the duration of interruptions. Software should be designed to minimize the impact of errors caused by communications failures.

Determine if ADP operations could be interrupted by the failure of other supporting utilities such as water, natural gas, steam, elevators or mail conveyors. If necessary, take steps to increase reliability and decrease the mean time to repair.

VI. Optimize Computer Reliability

Perform a failure analysis to estimate the number and duration of significant hardware failures and their impact on ADP operations. Estimate the annual loss expectancy from delays in performing urgent ADP tasks. Where cost is justified, increase system reliability by adding peripherals, multiple configurations, etc. Review maintenance facilities. Record and analyze all hardware failures in order to identify failure trends promptly and optimize preventive maintenance.

VII. Provide Physical Protection

Identify critical ADP areas including the computer room, data control and conversion area, data file storage area, programmer's area, forms storage area, maintenance area, and mechanical equipment room, and then provide adequate physical protection and access control.

Protect against theft, vandalism, sabotage, espionage, civil disorder and other forced intrusions with improved lighting and intrusion detection systems, with physical barriers at doors, windows, and other openings, and with guards as required.

Control access to critical areas and ADP facilities with conventional or electronic door locks; supervision by guards or receptionists over movement of people and materials; administrative procedures (sign-in logs, identification cards or badges, property passes and shipping/receiving forms); and other regulations.

VIII. Add Internal Procedural Security

Determine potential targets for fraud, theft or misuse of resources by analyzing the work flow and the nature of ADP tasks performed. Incorporate procedures which will minimize exposure to loss. Such procedures may include (1) requiring cooperation between two individuals to perform critical tasks; (2) performing additional checks and bounds comparisons; (3) formalizing standards for high risk operations; and (4) independent quality control checks.

Designate critical positions in ADP management, system programming, program library control, input output control, exception processing, applications programming, data base management, quality control, internal audit and hardware maintenance and require appropriate pre-employment screening.

Train and supervise all ADP personnel to assure understanding of, and compliance with, internal controls.

Implement control and record keeping procedures for job initiation, scheduling and distribution of output to prevent unauthorized processing.

Control access to physical data files to assure that data integrity is maintained, storage media are protected, custody of data files is traceable and their unauthorized use is prevented. Manual and automatic audit trails should be utilized.

Establish policy and procedures for program and data file retention to satisfy requirements for (1) back-up operation; (2) compliance with applicable statutes and regulation; (3) audit and management review of operation; (4) statistical analysis of operations; and (5) resolution of data integrity problems.

Implement programming, testing and documentation standards which satisfy requirements for (1) audit capability; (2) automated acceptance testing; (3) control program maintenance; (4) quality controls on input data; and (5) non-dependence on an individual's knowledge of systems and programs.

IX. Plan For Contingencies

Compile a set of back-up plans which accommodate the expected range of emergency events requiring back-up operation. The objective of such contingency plans is to protect users of the ADP facility against unacceptable loss. Document performance specifications, operation instructions and technical requirements (system hardware and software, program and data files, and preprinted forms) for each emergency operation

Select and periodically use an emergency back-up off-site ADP facility. Participate in establishing their security program.

Provide protection for the source documents, input and output data and programs while using the off-site facility and in transit.

Establish procedures to assure that (1) current copies of needed back-up materials are retained at a secure off-site location; (2) adequate time is available from compatible off-site ADP facilities; and (3) back-up personnel will be available if needed.

Plan for reconstruction of the ADP facility following destruction including specifications of (1) floor space (quantity, live load rating, location, etc. by functional use); (2) partitions, electric power service, air conditioning, communications, security, fire safety, etc.; and (3) ADP hardware, office equipment and supplies.

Coordinate ADP emergency plans for fire, flood, civil disorders, etc. with the Facility Self-Protection Plan to ensure life safety, limit damage, minimize disruption to ADP operations, and expedite repair.

X. Develop Security Awareness

Determine the security training requirements for the ADP staff, senior management, building staff, etc.

Select and implement appropriate security awareness techniques such as (1) training lectures and seminars; (2) posters; (3) orientation booklets; (4) amendments to job descriptions making employees responsible for security; (5) publicity for local security incidents, as well as others occurring at similar installations; and (6) rewards for employees who prevent breeches in security.

Establish and publicize punitive measures.

XI. Audit Physical Security

Establish an internal audit team with representatives from the agency's audit, building safety and security, ADP, and users' organizations.

Develop an audit plan and schedule which systematically validates all critical security and emergency measures.

State in the audit report which measures require improvement or replacement. Use a check sheet (problem description, responsibility for action, action required and follow-up) for each major deficiency to assure prompt resolution.

1. ADP Security Analysis

1.0. Introduction

The word **security** when applied to automatic data processing (ADP), is often taken to mean protection against wrongful disclosures or alternatively as protection against an aggressive attack on an ADP facility. However, Webster* defines **secure** as ". . . not likely to fail or give away; firm; strong; stable . . .". These are certainly desirable characteristics for an ADP facility and they are included in the broader meaning of security that this handbook addresses. It is intended to assist ADP managers and supporting agencies in defining specific ADP physical security requirements, developing and implementing sound physical security programs, and establishing and conducting audits of these programs. Those who are users of ADP facilities can avail themselves of this handbook to evaluate the security of those facilities, to participate effectively in security planning and to plan for adequate back-up. A Federal ADP facility exists to support the accomplishment of the missions of its parent agency and other users. The objective of the physical security program is to see that all reasonable steps have been taken to prevent situations which would interfere with mission accomplishment, in other words, to operate an ADP facility that is "not likely to fail."

1.1. Scope

The scope of the handbook is defined in detail in section 1.2, but generally speaking, it is concerned with physical effects or situations which affect the ADP facility. Measures to achieve controlled accessibility, a term defined in the "Controlled Accessibility Bibliography" [46][1] as the use of technological measures of hardware and software in a computer system to protect data against unauthorized access, have been excluded from this handbook. Privacy and confidentiality are defined as concepts which have to do with the nature of the data and who is authorized to have access. It should be understood, however, that it is difficult to place rigid boundaries on the various aspects of ADP security. A given measure will often achieve more than one objective. More than one discipline or function often will be required to deal effectively with a particular requirement, and so it is important to take a broad view of the subject during the study and planning stages.

The term **ADP security planner** is used here as a convenient title for the person(s) responsible for ADP security planning, but this should not be taken to mean that any one person can be expected to be competent in every area. Indeed, at each appropriate point sources of special knowledge are recommended. The manager of an ADP facility will derive the most from this handbok if he designates security as an on-going operational function, and provides adequate staff and budget to support the function.

The procedure suggested here for developing and implementing a physical security program can be summarized as follows:

- Analyze risk as the basis for development of a security policy.
- Select and implement appropriate security measures to reduce exposure to losses.
- Develop contingency plans for back-up operation, disaster recovery and emergencies.
- Provide indoctrination and training for personnel.
- Plan and conduct continuing tests and audits and adjust security measures and contingency plans as needed.

---

* Webster's New World Dictionary, 1957, The World Publishing Co., Cleveland.

[1] Figures in brackets indicate literature references in Appendix B at the end of this handbook.

1.2. Threats to ADP Operations

This handbook deals with the threats to ADP property and capital equipment and the physical hazards to continuing operation as outlined below:

Unauthorized access by people to specific areas and equipment for the purpose of committing acts such as theft, arson, vandalism, tampering, circumvention of internal controls, or improper physical access to information. These controls may include physical barriers such as fences or partitions, locked doors, receptionists or guards at control points, electronic devices such as closed circuit television and intrusion detectors, administrative procedures such as restricted access, and special identification badges.

Measures to minimize interruptions to data processing operations caused by ADP **hardware failures.** These measures may include introduction of redundancy in critical portions of the hardware configuration, preventive maintenance, and close monitoring and analysis of the causes of hardware failures.

Failure of supporting utilities including electric power, air conditioning, communications circuits, elevators or mail conveyors. Protective measures may include redundancy of critical elements, close monitoring or performance, physical protection against tampering or natural disasters and provision of means for prompt repair.

Natural disasters including floods, windstorms, fires and earthquakes. Countermeasures include careful selection of the site for the ADP building, details of building design and construction and provision of means to protect against the effects of emergencies.

Protection against **human errors** through effective use of training, supervision and controls to minimize errors.

Nonavailability of key personnel guarded against by cross-training for critical positions.

Neighboring hazards such as close proximity to chemical or explosive operations, airports, high crime areas or the like. Protection may include site selection, building design features, exclusion of such hazards from the ADP facility building and emergency planning.

Tampering with input, programs, or data files for fraudulent purposes. In addition to physical access controls, internal controls and procedures (which may also protect against errors) are used to deter or detect such tampering.

Compromise of data through **interception of** acoustical or electromagnetic **emanations** from ADP hardware. Countermeasures include isolation of ADP hardware from potential locations of interception equipment, shielding of ADP hardware or the room in which it is located and filtering of power lines. (It is not within the purview of this handbook to deal with interceptions through wiretapping or other compromise of data communications circuits.)

Of course, not every ADP facility will be faced with all of these threats. The impact of a given threat may depend on the geographic location of the ADP facility (earthquakes), the local environment (flooding), the potential value of property or data to a thief (blank check stock or information of value to a commodities speculator), or the perceived importance of the agency to activists and demonstrators or subversives.

1.3. Risk Analysis

Experience has shown that a quantitative risk analysis will produce the following benefits:

- Objectives of the security program are directly related to the missions of the agency.
- Those charged with selecting specific security measures have quantitative guidance on the amount of resources which it is reasonable to expend on each security measure.
- Long range planners will have guidance in applying security considerations to such things as site selection, building design, hardware configurations and procurements, software systems and internal controls.
- Criteria are generated for designing and evaluating contingency plans for back-up operation, recovery from disaster and dealing with emergencies.
- An explicit security policy can be generated which identifies what is to be protected, which threats are significant and who shall be responsible for execution, review and reporting of the security program.

For all these reasons, it is recommended that the ADP facility management begin development of the security program with a risk analysis. A suggested procedure is outlined in the sections which follow.

1.3.1 Loss Potential Estimate

The first step of the risk analysis is to estimate the potential losses to which the ADP facility is exposed. The objective of the loss potential estimate is to identify critical aspects of the ADP facility operation and to place a dollar value on the loss estimate. Losses may result from a number of possible situations:

Physical destruction or theft of tangible assets. The loss potential is the cost to replace lost assets and the cost to the user of delayed processing.

Loss of data or program files. The loss potential is the cost to reconstruct the files either from back-up copies if available or from source documents and possibly the cost to the user or delayed processing.

Theft of information. The loss potential here is difficult to quantify. Consider for example information gathered, collated and then publicly disseminated which affects marketplace activity. Knowledge of such information prior to dissemination would give a trader an advantage over others who would in effect sustain a loss equal to the trader's gain. Although the agency itself would sustain no direct loss it clearly would have failed in its mission. In some cases information itself may have market value as, for example, a proprietary software package or a name list which can be sold.

Indirect theft of assets. If the ADP system is used to control other assets such as cash, items in inventory or authorization for performance of services, then it may also be used to steal such assets. The loss potential would be the value of such assets which might be stolen before the magnitude of the loss is large enough to assure detection.

Delayed processing. Presumably every application has some time constraint on it and failure to complete it on time will cause a loss. In some cases it may be relatively easy to estimate the potential loss. For example, a failure to process payment checks promptly would prevent the exercise of a prompt payment discount under a procurement contract. Likewise, delays in an inventory system may lead to idle manpower at a warehouse, with secondary losses to recipients of materials stored at the warehouse, such as the cost of idle labor at a construction site. In other cases the loss potential may not be as obvious as, for example, a delay in issuing paychecks. Sometimes it may be helpful to use the daily operating cost of an agency as a rough rule-of-thumb estimate of the cost of delayed processing in those situations where a delay would more or less halt operations of an agency.

It should be noted that the loss experienced will in general increase with the duration of the delay. Therefore it is important to establish the maximum "no loss" delay time and an estimate of the median time to reconstruct the ADP facility after total destruction. Delay loss estimates, where losses are significant, should then be made for a range of delay durations between these two bounds. Generally three or four such representative durations will be adequate to establish loss trends.

The estimate of physical destruction loss potential is quite straightforward. The ADP security planner with the help of the building manager and procurement division should construct a table of replacement costs for physical assets of the ADP facility. This will usually include the following:

The building itself.

Special equipment installed to support the ADP facility such as air conditioning, electric power distribution, raised floor.

ADP hardware and other special equipment such as decollators, microfilm processors, keypunches.

Supplies and materials such as magnetic tapes, disk packs, forms, ribbons.

Office equipment such as desks, chairs, file cabinets, shelves, typewriters.

Preparation of this tabulation, broken down by specific areas, with help to identify areas needing special attention. While the contents of the typical office area may be valued at $5 to $10 per square foot, it is not unusual to find that the contents of a computer room are worth $500 to $2000 per square foot. The estimate will also be helpful in planning for recovery in the event of a disaster as described in section 8.4.

The remaining four loss potential types listed above are dependent on the characteristics of the individual data processing tasks performed by the ADP facility. The ADP security planner should review each task to establish which losses it is exposed to and which factors affect the size of the potential loss. Undoubtedly, he will want to call on users to help make these estimates, since it is unlikely that he will be aware of all loss factors.

In order to make the best use of time, the ADP security planner may want to do some kind of rapid, preliminary screening in order to identify the tasks which appear to have significant loss potential. For example, he might construct a table of preliminary estimates like the following very simple example:

Task Name	Run Time	File Reconstruction	Sensitive Data	Proprietary Data	Assets Controlled	No Cost Delay
P	1.5/D	Easy	No	Yes	Cash	One day
Q	On line	Very Diff.	No	No	None	2 hours
R	2.5/D	Difficult	Yes	No	Cash	8 hours
S	2.0/W	Uses P files	No	No	None	One week
T	0.5/D	Very Easy	Yes	No	Inventory	4 days

In this example task P runs 1.5 hours per day, has files that are easy to reconstruct, has no sensitive data, but does have proprietary data, controls cash and appears on first inspection to be able to be delayed up to one day without significant cost. In actual practice, the ADP security planner would provide much more detail: what files are used and why they are easy or difficult to reconstruct, what data is proprietary and how much cash is processed.

Having made the above analysis, he can then draw these initial conclusions:

Loss Exposure

Task	Loss of Data	Theft of Info.	Theft of Assets	Delayed Processing
Q	Yes	No	No	Extreme
R	Yes	Yes	Yes	Moderate
P	No	Yes	Yes	Moderate
T	No	Yes	Yes	Low
S	No	No	No	Very Low

Notice that on a judgmental basis, he has rearranged the tasks in descending order of sensitivity. Tasks Q and R should probably receive early attention and detailed evaluation. Task S appears to have a low loss potential and probably will require litle more than confirmation of the preliminary appraisal.

Having made a preliminary screening to identify the critical tasks, the ADP security planner should seek to quantify their loss potential more precisely with the help of user representatives familiar with the critical tasks and their impact on other activities. He should think about what could go wrong and how losses could occur, under the assumption that if something can go wrong that it will. The fact that a given task has never been tampered with or used for an embezzlement is no assurance that it never will be. At this stage of the risk analysis, the ADP security planner should assume the worst. Later he will undertake to estimate probability of occurrence, but at this point he wants to identify all of the significant potential losses so that each of them will be addressed by the security program.

1.3.2. Threat Analysis

The second step of the risk analysis is to evaluate the threats to the ADP facility. Threats and factors which influence their relative importance have been outlined in section 1.2. Details of threats are given in the chapters which follow and, to the extent it is available, general information about the probability of occurrence is given. These data and the application of common sense should be used by the ADP security planner to develop estimates of the probability of occurrence for each threat type.

While the overall risk analysis should be conducted by the ADP security planner, others can contribute to the threat analysis and their help should be solicited. The following is a list of threats and suggested sources of help in analyzing them:

Threat	Sources of Information	Refer to section
Fire	Building fire marshal and local fire department	2.1
Flood	Army Corps of Engineers	2.2
Earthquake	National Earthquake Information Center	2.3
Windstorm	National Oceanic and Atmospheric Administration and local National Weather Service Office	2.4
Power Failure	Building engineer and local public utility	3.1
Air Conditioning Failure	Building engineer and air conditioning vendor	3.2
Communications Failure	Federal Telecommunications System, building and local telephone company	3.3
ADP Hardware Failure	Hardware vendors and Federal Supply Service	4.0
Intruders, Vandals, etc.	Building manager, security director and the Office of Federal Protective Service Management, GSA.	5.0
Compromising Emanations	Hardware vendors and the Office of Federal Protective Service Management, GSA.	5.2
Internal Theft or Misuse	System Design, Internal Audit and Personnel Division	6.0

1.3.3. Annual Loss Expectancy

The third step in the risk analysis is to combine the estimates of the value of potential loss and probability of loss to develop an estimate of annual loss expectancy. The purpose is to pinpoint the significant threats as a guide to the selection of security measures and to develop a yardstick for determining the amount of money which it is reasonable to spend on each of them. In other words, the cost of a given security measure should relate to the loss(es) against which it provides protection.

To develop the annual loss expectancy, one can construct a matrix of threats and potential losses. At each intersection one asks if the given threat could cause the given loss. For example, one might decide that fire, flood and sabotage do not cause theft-of-information losses but that in varying degrees all three result in physical destruction losses and losses due to delayed processing. Likewise internal tampering could cause an indirect theft of assets. In each case where there can be significant loss, one multiplies the loss potential by the probability of occurrence of the threat to generate an annual estimate of loss.

As an example of a loss expectancy estimate, consider the simplified case where there are three ADP tasks in which loss could result from delays in completed processing as follows:

	Delay Duration			
Task	One Hour	Four Hours	Eight Hours	One Day
A	--	--	$10,000	$ 45,000
B	--	$ 5,000	12,000	55,000
C	$3,000	16,000	45,000	160,000
TOTAL	$3,000	$21,000	$67,000	$260,000

Further assume that the annual probability of each such delay duration resulting from electric power failures have been estimated to be 0.75, 0.31, 0.10 and 0.09 respectively. One could conclude that the annual loss expectancy from electric power failure would be:

0.75 × $3,000 + 0.31 × $21,000 + 0.10 × $67,000 + 0.09 × $260,000 = $38,860 per year.

The cost of power failures is relatively easy to estimate since both probability of occurence and effect on operations can be quantified with some precision. Air conditioning and communications failures also fall into this class. Quantifying fire losses is a different matter. One might deal with them by considering several degrees of severity and a number of loss types as shown in figure 1. The probabilities of occurrence come from the estimate of inherent fire safety in section 2.1 and the dollar losses are from the estimates of loss potential in section 1.3.1. A similar technique can be applied to earthquakes, floods, windstorms and similar natural disasters.

		Fire Description		
		Minor Fire in ADP Area	Major Fire in Bldg.	Total Loss Fire
Occurrence Probability		0.10	0.05	.0005
Potential Loss Types	Building Damage	$10,000	$100,000	$3,700,000
	ADP Hardware	50,000	10,000	2,100,000
	General Equip.	5,000	--	285,000
	Supplies, etc.	10,000	--	130,000
	Task D—Delay	--	--	35,000
	Task E—Delay	5,000	7,000	100,000
	Task F—Delay	12,000	20,000	250,000
	File Reconstruct	5,000	--	85,000
Total potential loss		97,000	137,000	6,685,000
Annual loss		$ 9,700	$ 6,850	$ 3,342

FIGURE 1. *Estimating fire loss.*

Human acts are more difficult to project since there is no easy way to estimate probability of occurrence. However, one can probably estimate potential losses with acceptable accuracy and so pinpoint critical threats. For example, consider fraud via program tampering. An examination of tasks which disburse funds might reveal the following:

Task	Dollars per Cycle	Expected Program Changes (next 12 months)
J	$20,000,000	5
K	200,000	25
L	5,000,000	10

If one assumed that a 1% theft would definitely be detected and also that the embezzler would not attempt to insert a wrongful program change more often than once in ten changes, one could draw these conclusions:

Task	Potential Theft	Fraud Expectation	Est. Loss
J	$200,000	0.5	$100,000
K	2,000	2.5	5,000
L	50,000	1.0	50,000
			$155,000

Such conclusions might appear improbable. Perhaps the assumptions are not valid. The judgment factor plays a large part in arriving at these conclusions; repeated attempts may serve to sharpen one's judgment in such matters. As a result of iterative analyses, one might arrive at an annual loss for J of $10,000, or twice that of K, and for task L a loss equal to that for K or $5,000; the revised annual loss potential for the three tasks then would be only $20,000.

The key point is that in attempting the estimate, a clearer picture of the critical exposures and reasonable criteria emerges. It now becomes obvious that task K is just as critical as task J because, even though it disburses only one hundredth as much money per cycle, the program is still in a fluid state and therefore more subject to compromise. Because a quantitative effort has been undertaken, the probability of occurrence of each threat and its effect on the ADP facility have been examined realistically.

Clearly this is not an exact science. Indeed, it is quite likely that one will have to reappraise threats and losses more than once, concentrating on the areas initially identified as most critical, before the loss expectancy estimate reaches a satisfactory level of confidence. In some cases it may not be feasible to generate more than a rough estimate; however, the value of disciplined thinking about risk will be ample reward for the effort to deal with it in a quantitative way.

1.3.4. Selecting Remedial Measures

When the estimate of annual loss has been completed, ADP management will have a clear picture of the significant threats and critical ADP tasks. The response to significant threats can take one or more of the following forms:

Alter the environment to reduce the probability of occurrence. In an extreme case this could lead to relocation of the ADP facility to a less exposed location. Alternatively, a hazardous occupancy adjacent to or inside the ADP facility could be moved elsewhere.

Erect barriers to ward off the threat. These might take the form of changes to strengthen the building against the effects of natural disasters, saboteurs or vandals. Special equipment can be installed to improve the quality and reliability of electric power. Special door locks, guards and intrusion detectors can be used to control access to critical areas.

Improve procedures to close gaps in controls. These might include better controls over operations, more rigorous pre-hire screening or standards for programming and software testing.

Early detection of harmful situations permit more rapid response to minimize damage. Fire or intrusion detectors are both typical examples.

Contingency plans permit satisfactory accomplishment of agency missions subsequent to a damaging event. Contingency plans will include immediate response to emergencies to protect life and property and to limit damage, maintenance of plans and materials needed for back-up operation off-site and maintenance of plans for prompt recovery following major damage to or destruction of the ADP facility.

The criteria for selecting specific remedial measures are that the annual cost of the remedial measures shall be less than the reduction in expected annual loss which they bring about and that the mix of remedial measures selected shall be the one having the lowest total cost.

The first criterion simply says that there must be a cost justification for the security program—that it returns more in savings to the ADP facility than it costs. This may seem obvious but it is not uncommon for an ADP manager to call for a security measure without first analyzing the risks. His experience and judgment tell him that some particular action is desirable. While this might seem to obviate the need for risk analysis, what it really amounts to is recognition of a possibly serious but unquantified loss potential. It would be more appropriate for the ADP manager to factor his judgment into a quantified risk analysis.

The second criterion reflects the fact that a given remedial measure may often be effective against more than one threat. To illustrate:

REMEDIAL MEASURES	THREATS				
	Fire	Internal theft	External theft	Hurricane	Sabotage
Fire detection system	X				X
Loss control team	X			X	X
Roving guard patrol	X	X	X		X
Intrusion detectors		X	X		X
Personnel screening		X			X
On-site power generator				X	X
Back-up plan	X			X	X

Since a given remedial measure may affect more than one threat, the least cost mix of measures probably will not be immediately obvious. One possible way to make the selection is to begin with the threat having the largest annual loss potential. Consider possible remedial measures and list those for which the annual cost is less than the expected reduction in annual loss. (Precision in estimating cost and loss reduction is not necessary at this point.) If two or more remedial measures would cause a loss reduction in the same area, list them all but note the redundancy. Repeat the process for the next most serious threat and continue until reaching the point where no cost justifiable measure for a threat can be found. When the cost of a remedial measure is increased if it is extended to cover an additional threat, the incremental cost should be noted. At this point one has a matrix of individual threats and remedial measures with estimates of loss reductions and costs and thus an estimate of the net saving, which can also be shown graphically:

REMEDIAL MEASURES	THREATS											
	A			B			C			D		
J	20*	9	11	10	0	10	4	1	3	2	5	—3
K	20*	15	5	12	0	12	6	0	6	4	2	2

* Same effect.

For each threat, the estimated loss reduction, the cost of the remedial measure and the net loss reduction have been given (in that order). By applying remedial measure J to threat A at a cost of $9,000, a loss reduction of $20,000 can be expected (a net saving of $11,000). Furthermore remedial measure J will reduce the threat B loss by $10,000 at no additional cost and the threat C loss by $4,000 at an added cost of only $1,000. Finally, though, it appears that it would cost more than it would save to apply J to threat D. Therefore J would not be implemented for D. The net loss reduction from J could be expressed as:

$$\begin{aligned} J\,(A, B\ \&\ C) &= 11 + 10 + 3 \\ &= \$24{,}000 \end{aligned}$$

The table indicates that J and K have the same reduction effect on threat A. Since K costs more than J, it might, at first glance, be rejected. However,

$$\begin{aligned} K\,(A, B, C\ \&\ D) &= 5 + 12 + 6 + 2 \\ &= \$25{,}000 \end{aligned}$$

and

$$\begin{aligned} J\,(A, B\ \&\ C) + K\,(A, B, C\ \&\ D) &= \\ -4 + 22 + 9 + 2 & \\ &= \$29{,}000 \end{aligned}$$

Therefore, while J and K are equally effective on threat A, K appears to be more effective than J on the other threats, but further checking shows that their combined use results in the greatest overall net loss reduction.

By going through the process just described, using preliminary estimates for cost and loss reduction, the ADP security planner can test various combinations of remedial measures. This will enable him to identify the subset of remedial measures which appears to be the most effective. At this point the ADP security planner should review the estimates for the candidate subset and refine them as necessary to establish confidence in the tentative choices. In marginal situations this might cause a change of the optimum subset. However, by iterating the process as required, the ADP security planner will finally reach the point where he can recommend a given group of remedial measures with considerable confidence. And, almost as important is the ability to defend the rejection of remedial measures which cannot be cost justified.

If all of the above procedures have been followed, the following will have been established and documented:

- Significant threats and probabilities of occurrence.
- Critical tasks and the loss of potential related to each threat on an annual basis.
- A list of remedial measures which will yield the greatest net reduction in losses, together with their annual cost.

With this information at hand ADP management can move ahead with implementation of the physical security program. Since the analysis of remedial measures will have identified those with the greatest impact, relative priorities for implementation can also be established.

1.4. Implementing the Security Program

In section 1.3 the use of a risk analysis has been described as the basis for developing an ADP security program. Implementation of the program will depend on local conditions and the practical constraints of time and budget, but it may not always be clear just where to begin. The following is a brief outline of a procedure which should be generally applicable.

- **Preliminary planning.** Establish an ADP security study team to prepare an ADP security program consisting of detailed task descriptions for the next three tasks, a budget and schedule and responsibility assignments.

- Perform a preliminary risk analysis to **identify major problem areas.**

- Select and implement urgent **"quick fix"** security measures as needed.

- Perform and document a detailed **risk analysis** for review and approval

- Based on the approved risk analysis selected, cost justify and **document action plans** with budgets and schedules for security measures, contingency plans, training and indoctrination plans and test and audit plans.

- **Carry out** the approved action plans.
- Depending on the results of tests, audits and changes in mission or environment, **repeat the detailed risk analysis** and subsequent steps on a regular, at least annual, basis.

The action plans should include adequate documentation. The documentation might include:

- A security policy statement which provides general guidance and assigns responsibilities.
- A security handbook which describes in detail the security program and procedures and the obligations of ADP personnel, users and supporting personnel.
- Technical standards for system design, programming, testing and maintenance to reflect security objectives.
- Contingency plans for back-up operations, disaster recovery and emergency response.
- Booklets for ADP staff indoctrination in security program requirements.

Depending on the normal practice of the ADP facility, these documents may be completely separate items or may be included in other documents. For example, emergency response plans for the ADP facility might be included in the agency's Facility Self-Protection Plan. Similarly, technical security standards could be added to existing documents.

The final point to be made is the importance of continuing audit and review of the security program. A major effort will be required for the initial risk analysis but once it has been completed a regular review and updating can be done much more quickly. By evaluating changes in agency mission, the local environment, the hardware configuration and tasks performed, the ADP security planner can determine what, if any, changes should be made in the security program to keep it effective.

1.5. Supporting Documents

There are a number of Federal documents relating generally to ADP security which will be helpful to security planners. These, as well as a number of other useful references, are listed in the bibliography in Appendix B. It is suggested that this list be consulted by planners early in their assignment in order to be able to take advantage of the extensive fund of knowledge they represent.

2. Anticipating Natural Disasters

2.0. Introduction

This chapter deals with fire, flood, windstorm and earthquake. These events all tend to have the same basic effects on ADP operations: physical destruction of the facility and its contents and interruption of normal operations. They also represent a threat to the life safety of the ADP staff. In the sections which follow, protective measures and factors for evaluating exposure are presented. Planning for emergency response is discussed in Chapter 8—Contingency Planning.

2.1. Fire Safety

Experience over the last two decades has demonstrated the sensitivity of ADP facilities to fire damage and disruption of operations. For example, a parts warehouse which included a $1 million computer system was totally destroyed by a fire. The building, almost 0.8 sq mi (two hectares) in size, was of non-combustible construction and had neither sprinklers, interior fire partitions nor fire curtains. Furthermore, the building was located just outside the municipal fire district, presumably because of the low tax rate. The fire evidently started when an electric spark ignited a flammable solvent being used to remove floor sealant. Although the structure, contents and computer system were completely destroyed, the company's emergency procedures called for storage of magnetic tapes in fire-rated vaults and they were recovered intact. As a result, and with a major effort on the part of the hardware vendor, a new computer system was operating at an alternate site four days later. This episode highlights the value of close attention to both fire safety and contingency planning. A number of such major losses have involved noncombustible buildings. In those cases where vital tapes had been safeguarded and the computer hardware was relatively uncomplicated, rapid recovery was possible, often in a matter of days. However, it seems likely that if a large computer configuration is destroyed or if back-up records are inadequate, recovery would be a lengthy process that could take many weeks or months.

Fire safety should be a key part of the ADP facility physical security program and should include these elements:

- Location, design, construction and maintenance of the ADP facility to minimize the exposure to fire damage.
- Measures to insure prompt detection of and response to a fire emergency.
- Provision of adequate means to extinguish fires and for quick human intervention.
- Provision of adequate means and personnel to limit damage and effect prompt recovery.

Each of these points is discussed in the subsections which follow. A comprehensive treatment of the subject of fire prevention and control is also the subject of the Fire Protection Handbook [24]. To quote from the handbook itself, it ". . . constitutes an authoritative encyclopedia on fire and its control and is designed to serve both as a textbook for those learning the science and as an independent reference book . . .". It includes fire control considerations in building design and construction, tables of the fire hazard properties of several hundred materials, and an engineering handbook on hydraulic properties, in addition to the other topics on fire control one would expect in such a handbook.

2.1.1. ADP Facility Fire Exposure

The first factor to consider in evaluating the fire safety of an ADP facility is what fire exposure results from the nature of the occupancy of nearby buildings and the ADP facility building Generally speaking the degree of hazard associated with a given occupancy depends on the amount of combustible materials, the ease with which they can be ignited and the likelihood of a source of ignition. The following occupancies have been found to be particularly hazardous: building under construction; clothing and textile processing; chemical, plastic, paint and petroleum processing; electric appliance assembly; foundries; paper manufacturing; and storage and warehousing operations. The inherent hazard of an occupancy can also be evaluated in terms of the probable severity of a fire as a function of the heat potential (fuel load) of the contents. This relationship can be expressed approximately as follows:

Fuel Loading (Equivalent pounds of wood per square foot)	Potential Heat Release Kilocalories per square centimeter)	Fire Severity (duration in hours)
5	11	0.5
10	22	1
20	43	2
30	65	3
50	110	6
70	152	9

A typical office with metal furniture and storage cabinets will have fuel loading ranging from 5 to 15 pounds per square foot (11 to 33 kcal/cm^2). A storage room for paper forms and boxed punched cards, or a magnetic tape library, will have fuel loads of 50 to 80 pounds per square foot (110 to 175 kcal/cm^2).* The severity of a fire and its effect on the structure and contents will depend on the rate at which temperature rises and the duration of the fire. Thus if the fuel load is so configured and stored as to retard ignition and combustion of, for example, paper records in metal file cabinets, temperature will rise relatively slowly. If the same fuel load were in the form of reels of magnetic tape stored in relatively open racks, the temperature could be expected to rise rapidly but the fire would be of brief duration.

The second fire safety factor is the design and construction of the building. There are five basic types of construction:

- **Fire-Resistive**—The structure of the building—framing, floors, walls and roof—is constructed of noncombustible materials which are insulated to protect against loss of strength as a result of a fire.
- **Heavy Timber**—Exterior walls are noncombustible with a 2-hour rating and columns, beams, floors and roof are heavy timber. Because of the slow burning character of heavy timber, it will be superior in performance to noncombustible.
- **Noncombustible**—The structure is noncombustible, but lacks protection against the effect of heat on the structural members. The difference is this: while a fire in a noncombustible building will not draw fuel from the structure itself, the heat from the fire may cause the structure to collapse. A classic example of a noncombustible building fire was a transmission plant in Michigan. Although the structure itself did not contribute any fuel to the fire, the asphalt on the roof provided enough fuel to completely destroy the building.
- **Ordinary Construction** — Ordinary construction is the same as Heavy Timber except that the dimensions of the timber portions of the structure are too small to qualify as heavy timber.

---

* NFPA computes fuel load based on a heat of combustion of 8,000 BTU per pound: a representative value for wood or paper. Magnetic tape is roughly twice as combustible as wood, so that 40 lb of magnetic tape would have an 80 lb fuel load.

- **Wood Frame**—This is the typical residential construction using two inch (5 cm) thick framing and one inch (2.5 cm) boards.

To summarize the above simply, and ignoring design features which can increase fire resistance, one can construct the following table:

Type of Construction	Approximate Fire Classification
Fire Resistant	2 or 3 hours
Heavy Timber	1 plus hours
Noncombustible	1 hour
Ordinary Construction	Less than 1 hour
Wood Frame	Minutes

The actual performance of a building will depend not only on the type of construction, but on design details such as:

- **Fire walls** which in effect divide a structure into separate buildings with respect to fires.
- Fire rated **partitions** which retard the spread of a fire within a building.
- Fire rated **stairwells, dampers or shutters** in ducts, fire stops at the junction of floors and walls and similar measures to retard the spread of smoke and fire within a building.
- Use of **low-flame-spread materials** for floor, wall and ceiling finish to retard propagation of flame.

To summarize, the four basic fire safety factors and their effects can be tabulated as follows:

Factor	Effect
Occupancy	Probability of a fire occurring
Fuel load	Intensity and duration of a fire
Construction Type	Resistance to structure damage
Construction Details	Confinement of a fire

It should be understood that this discussion has been much simplified. However, consideration of these factors by the ADP security planner as they apply to an existing or projected ADP facility will help him to determine the amount of attention he should pay to fire safety. He will want to seek the assistance of a qualified fire protection engineer in evaluating the inherent fire safety of the ADP facility and identifying hazards. A detailed discussion will be found in "Building Firesafety Criteria" [13].

The July, 1973 fire at the U.S. Military Personnel Records Center, Overland, Mo., was an unfortunate demonstration of the result when well tested fire safety design criteria are disregarded in overemphasizing protection against other risks. Lack of sprinkler protection, inadequate access to the fire site and related design deficiencies seriously hampered fire fighting and in the end resulted in much more damage to records than would have resulted from the operation of sprinkler heads.

The third factor in fire safety is the way in which the building is operated. It should be understood that the inherent fire safety of a building can be rendered ineffective by careless operation. This includes: fire doors propped open; undue accumulation of debris or trash; careless use of flammable fluids, welding equipment and cutting torches; substandard electric wiring; inadequate maintenance of safety controls on ovens and boilers; and excessive concentration of flammable materials. ADP facilities, for example, have a particular hazard from the accumulation of lint from card and paper operations. The ADP physical security program should strive, in coordination with the building maintenance staff, to identify and eliminate such dangerous conditions. Furthermore, it should be understood that this must be a continuing effort and a consideration in the assignment of security management responsibilities. The security audit plan should include verification of compliance with established standards.

Specific guidance for the construction of ADP facilities will be found in chapter 2 of "Fire Protection for Essential Electronic Equipment" [9]. This document, hereafter referred to as RP-1, has been adopted by the GSA for all GSA facilities under GSA Order PBS 5920.4B with certain minor modifications.

2.1.2. Fire Detection

Despite careful attention to the location, design, construction and operation of the ADP facility, there is still the possibility that a fire can start. Experience has shown repeatedly that prompt detection is a major factor in limiting fire damage. Typically a fire goes through three stages. Some event, such as a failure of electrical insulation, causes ignition. An electrical fire will often smolder for a long period of time. When an open flame develops, the fire spreads through direct flame contact, progressing relatively slowly, with a rise in the temperature of the surrounding air. The duration of this stage is dependent on the combustibility of the materials at and near the point of ignition. Finally the temperature reaches the point at which adjacent combustible materials give off flammable gases. At this point the fire spreads rapidly and ignition of nearby materials will result from heat radiation as well as direct flame contact. Because of the high temperatures and volumes of smoke and toxic gases associated with this third stage, fire fighting becomes increasingly difficult and often people cannot remain at the fire site.

Given the objective to discover and deal with a fire before it reaches the third stage, one can see the limitation of fire detection which depends on detecting a rise in air temperature. It is for this reason that RP-1 requires that the areas in which electronic equipment is installed be equipped with products-of-combustion (smoke) detectors. Such detectors use electronic circuitry to detect the presence of abnormal constituents in the air which are usually associated with combustion.

To be effective in providing prompt detection the following points should be considered in designing a fire detection system:

- The **location and spacing of detectors** should take into consideration the direction and velocity of air flow, the presence of areas with stagnant air, and the location of equipment and other potential fire sites. Note that detectors may be required under the raised floor, above the hung ceiling and in air conditioning ducts as well as at the ceiling. It may also be wise to put detectors in electric and telephone equipment closets and cable tunnels.

- The **design of the detection control panel** should make it easy to identify the detector which has alarmed. This implies that the detectors in definable areas (for example, the tape vault, the east end of the computer room, etc.) should be displayed as a group on the control panel. In other words, when an alarm sounds, inspection of the control panel should indicate which area or zone caused the alarm. Generally, and preferably, each detector will include a pilot light which lights when the detector is in the alarm state. In some cases it may be determined that there should be a separate indicator light at the control panel for each detector. It is also important to see that the alarm system itself is secure. Its design should cause a trouble alarm to sound if any portion of it fails, or if there is a power failure. Steps should be taken to assure that the system could not be deactivated readily, either maliciously or accidentally. In a recent case of suspected arson in a tape library it appeared that the smoke detection system had been turned off.

- **Meaningful human response** to the detection and alarm systems is necessary if they are to be of any value. This means that the fire detection system should be designed to assure that someone will always be alerted to the fire. Typically, we expect that the computer room staff will respond to an alarm from the ADP facility alarm system. A remote alarm should also be located at another point in the building which we expect will be manned at all times, such as the lobby guard post, security center or building engineer's station. This provides for back-up response and response when the computer area is not occupied. If there is any possibility that the remote alarm point will not be manned at all times, a third alarm point should be located off-site, typically at the nearest fire station or location of the fire brigade for the facility.

- **Proper maintenance** is essential to the fire detection system. The nature of smoke detectors is such that nuisance alarms may be caused by dust in the air or other factors. Thus there is a tendency to reduce sensitivity in order to eliminate nuisance alarms, with the result that detection of an actual fire may be delayed. To insure proper operation, it is important to see that qualified personnel (a vendor representative or building engineer) verify correct operation at the time of installation and at least once each year thereafter. Furthermore, each fault condition should be corrected immediately. Unfortunately, there is a common tendency to turn off the fire detection system or silence the alarm bell, creating the danger that there will be no response if a fire should occur.

In addition to alerting personnel to the presence of a fire, the detection equipment can be used to control the air conditioning system. There is some support for the view that upon detection, air handling equipment should be shut down automatically to avoid "fanning the flames" and spreading smoke. This may not be the best plan, as nuisance alarms will result in needless disruption. A preferred technique may be to cause the system to exhaust smoke by stopping recirculation and switching to 100% outside air intake and room air discharge. As a rule this can be done by adjustment of air conditioning damper controls and their interconnection with the fire detection system. However, it may be necessary to modify the air conditioning system. More details will be found in section 3.2.

2.1.3. Fire Extinguishment

Fire extinguishment is accomplished in four ways:

- **portable or hand extinguishers** operated by agency personnel in an effort to control the fire before it gets out of hand.

- **hose lines** used by professional fire fighters to attack the fire with water.

- **automatic sprinkler systems** which release water from one or more sprinkler heads when the air temperature reaches the design temperature of the head which range from 135-280 °F (57-138 °C).

- **volume extinguishment systems** using HALON-1301* which fill the room with a gas that interferes with the combustion process.

A review of the history of fires involving electronic equipment and the effectiveness of each of these extinguishment devices has led the Federal Fire Council to establish a number of requirements for extinguishment in Chapter 3 of RP-1.

First, at least one carbon dioxide extinguisher of 15 pounds (6.8 kg) capacity or more and one 2½ gallon (9.5 l.) plain water extinguisher shall be located within fifty feet (15 m) of each piece of equipment. These extinguishers are intended to be used by ADP facility personnel for immediate fire fighting. Given prompt detection and response by properly trained personnel and freedom from gross fire hazards in the computer area, portable extinguishers will be effective for controlling most fires quickly.

To insure effectiveness of portable extinguishers, several points must be considered. Extinguishers should be placed in readily accessible locations, not in corners or behind equipment. Each location should be marked for rapid identification; for example, a large red spot or band can be painted on the wall or around the column above the point where each extinguisher is mounted. It is important to have all extinguishers inspected. (See "Portable Fire Extinguishers" [44].) Each extinguisher should have an inspection tag affixed to it on which the inspector signs his name and gives the inspection date. In addition to the required extinguishers, it may be wise to provide five pound (2.3 kg) carbon-dioxide extinguishers in areas principally staffed by personnel unable to lift heavy objects. Experience indicates that such personnel can deal effectively with minor equipment and trash fires if lighter extinguishers are made available to them.

The second RP-1 requirement is that computer areas be equipped with automatic sprinklers and, unless building construction is fire resistive or noncombustible, that the entire building shall be so equipped. Portions of the building which are not protected by sprinklers and which cannot be reached easily with hose lines from the exterior should have standpipes and inside hose systems. The automatic sprinkler system is the preferred extinguishment system for a number of reasons, but the ADP facility manager may be concerned that installation of sprinklers will expose the ADP facility to serious water damage. If the worst thing that could happen to an ADP facility were to spray water on the hardware, it would make sense to omit sprinkler protection, but it isn't; the worst is a structural collapse of the building. In an effort to provide effective extinguishment without damaging side effects, one might consider a HALON-1301 deluge system. Carbon dioxide (CO_2) systems represent a significant life safety hazard and their use cannot be recommended. The characteristics of automatic sprinklers and HALON-1301 are compared below:

	Automatic Sprinklers	HALON-1301
Extinguishment mechanism	Water cooling and smothering of fire site.	Chemical interference with combustion process.
Reliability	Very high; limited by reliability of water supply.	Very high; limited by reliability of detection system.
Effectiveness	Very high.	Very high if effective concentration is achieved at fire site.
Life safety hazard	None.	Some danger if concentration greater than 10%.
Side effects	Prompt cooling and cleaning of air by water spray with attendant damage to contents.	No side effects if effective; otherwise corrosive toxic decomposition products.
Approx. cost to install	$1.00/sq. ft. new building, $3.00+/sq. ft., retrofit.	$0.50/cu. ft. of protected volume.
Discharge controlled by:	Air temperature (or auto. recycle)	Detection system or manual.
Time and cost to refurbish after fire	Minutes and $5 to $20.	Hours and 40% of installed cost.

Because of its lower cost, proven effectiveness and inherent safety, the automatic sprinkler is the preferred fixed extinguishment system in most cases. HALON-1301 appears to be better suited for the initial fire attack at critical points, such as a tape or disk storage area or a room housing one-of-a-kind hardware or at points which cannot be covered effectively by a sprinkler system, e.g., under a raised floor or in a cable tunnel.

---

* HALON—1301 is a term applied to bromotrifluoromethane, a halogenated extinguishing agent.

Automatic sprinkler systems offer a feature which should be included in the fire safety system. Devices called flow sensors are available which can be inserted into the sprinkler pipes to detect the flow of water. These flow alarms should be located at the source of water and at each major branch in the piping and should be connected to a fire alarm panel. When a fire causes a sprinkler head to open and discharge water, an alarm will be sounded alerting personnel to the emergency. This feature can be of real value during hours when work areas are unoccupied, as the security force is alerted immediately to sprinkler operation and can shut off the water flow as soon as the fire is extinguished. To make this easy to do, the sprinkler system piping should be configured to supply the computer area from a single point and equipped with a shut-off valve which is located in an easily accessible point. All sprinkler system shut-off valves should have supervisory switches attached which will signal the fire alarm panel if a valve is closed. This is important because there have been many cases where fires were not defeated because sprinkler control valves had been left closed inadvertently. In some cases it was suspected that valves were closed deliberately.

The gas extinguishment systems also have features which contribute to more effective and reliable quenching. Pressure sensors are used to detect a significant loss of gas and to signal a trouble alarm. Systems are normally installed so that there is a delay of up to a minute between the initial alarm and release of the gas. With carbon dioxide systems, this allows the area to be clear of personnel, because of the serious hazard to life when the gas is discharged. With HALON systems, the delay permits the actual discharge of this rather expensive quenching agent to be overridden manually when there is no fire or when the fire is quenched easily by using portable extinguishers.

If fire extinguishing equipment is to remain effective, it must have regular maintenance by properly qualified personnel. "Fire Extinguishing Equipment" [11] is a useful guide to extinguisher equipment inspection and maintenance. The ADP security planner should work with the Building Manager and Fire Marshal to insure that an effective maintenance program is in effect. The bibliography lists a number of standards, guidelines and recommendations from the National Fire Code published by the National Fire Protection Association [22-43].

2.1.4 Fire Fighting

The discussion of extinguishment has stressed the value of prompt, effective fire fighting. With regard to who should do this fire fighting, the ADP facility manager should consider local conditions carefully to determine the most practical approach to meet this individual problem. Some ADP facilities are located within large industrial complexes which either employ their own professional firefighters, have highly trained industrial fire brigades or are located in close proximity to a municipal fire department composed of professional firefighters. Conversely, some facilities may be situated in remote locations where response by professional or highly trained firefighters is delayed or perhaps nonexistent because of travel distance. Obviously, the best arrangement is one which results in immediate response by professional firefighters in time of need. However, when this is not feasible, other alternatives must be explored—particularly when one considers the high value of equipment usually housed within ADP facilities.

In all probability, the enlightened ADP facility manager will want to establish a first line of defense against fire involvement between the time of notification of and response by professional or highly trained firefighters, and will incorporate this as part of the Facility Self Protection Plan. Every plant, regardless of size, needs personnel who are knowledgeable and trained in fire safety. Any practical and effective organization for fire protection must be designed to assure prompt action immediately at the point where a fire breaks out. This usually necessitates every organizational unit or area of a plant having a nucleus of key employees who are prepared through instruction and training to extinguish fires promptly in their incipient stage. Such individuals become knowledgeable in specialized fire protection and the systems applicable to the facility in question: how to turn in an alarm, which type of extinguisher to use for which type of fire and how to use it. Further, such individuals can serve as on-the-job fire inspectors, constantly seeking out and reporting and correcting conditions that may cause fires. They can help ensure that fire fighting equipment is properly located and maintained, that storage does not cause congestion which could hamper fire fighting, and that general housekeeping is maintained at a reasonably high level to minimize fire risk.

Should a decision be made to establish an ADP facility fire brigade organization, reference should be made to the NFPA "Industrial Fire Brigades Training Manual" [27]. This document will serve as a useful guide in organizing and training a fire brigade. The ADP fire brigade should consist of a fire captain, a deputy fire captain and several fire fighters on each operating shift. Large ADP facilities should consider more fire fighters to ensure adequate coverage. All other members of the facility staff should vacate the premises during fire involvement.

Designated fire fighters should receive training each year in extinguishing actual fires using extinguishers of the type located in the computer area. In addition, they should understand the operation of fire detection equipment, alarms, sprinklers and any other fire safety equipment. To maintain competence, the fire brigade should meet regularly, perhaps at two or three month intervals, for brief training sessions. The fire captain should review any new equipment or procedures. He might also lead a discussion about how to deal with a hypothetical fire situation with questions like: What equipment should be turned off? Where is the nearest extinguisher? Other nearby extinguishers? Would there be any difficulty in getting at the fire site? Who is notified and how? He should also ask for discussion of newly-observed fire safety problems. Undoubtedly the building fire marshal and the local fire department can and will contribute to the training program with training materials and facilities and with advice.

Because of the special characteristics of ADP hardware and the desire to avoid disruption to operations, it is important for fire fighting and loss control measures to be carefully structured. ADP management and systems and operations supervisors should participate with the fire marshal and fire captains in developing guidelines for decisions to power down hardware, shut off air conditioning and take related steps. All fire control measures must be coordinated with the fire department serving the ADP installation. There should be site visits to familiarize the fire department with normal and emergency entrances, electric power switches, hoses and portable extinguishers, sprinkler control valves, location of covers for equipment, exhaust fans and ventilation controls, combustibles storage, building construction and characteristics, and other pertinent items. Unique ADP hazards such as the susceptibility of disk and drum surfaces to contamination and the presence of underfloor electric outlets should be pointed out.

Emergency planning is presented in more detail in Chapter 8.

2.2. Flood

The discussion of automatic sprinklers in the preceding section may have left the impression that water damage can be dismissed as a significant threat to ADP facilities. While it is true that the damage resulting from operation of one or two sprinkler heads will be minor and certainly preferable to the smoke and heat damage of a major fire, flooding is quite a different matter. The water may be contaminated with dirt, oil or chemicals. Buildings may be damaged or even destroyed.

Tropical storm Agnes which swept through Pennsylvania in June, 1972, caused severe flooding. Newspaper accounts reported that hundreds of computer systems were submerged in mud and water. The resulting damage appeared to depend largely on location and the reported time to recover ranged from two days to two months. The Pennsylvania Bureau of Management Information Systems reported its large computer submerged in six feet of water. The entire reserve supply of certain forms used weekly, 45 million in all, was lost by another computer facility, leaving only a one week supply on hand. A number of computer centers lost card data files which were not backed up.

This experience points up two things. First, if an ADP facility is located in a basement in a low lying area, disruptions from flooding are almost inevitable. Second, careful planning for back-up operation can greatly reduce the time required to restore normal operations after an emergency.

Executive Order 11296 was issued in August 1966 in response to growing concern about flood-related losses in Federal buildings but to insure optimum use of flood plains by Federal agencies. In summary this Executive Order requires executive agencies to evaluate flood hazards when locating new facilities, administering funds to support facilities, evaluating future use of Federal facilities to be disposed of, or when planning land use so as to "preclude the uneconomic, hazardous, or unnecessary use of flood plains . . .". Where practical and economically feasible, it requires that flood-proofing measures be applied to existing structures.

Flood hazard information is available primarily from the Army Corps of Engineers, the Tennessee Valley Authority and also from the Departments of Agriculture, Interior, Commerce, Housing and Urban Development and from the Office of Emergency Planning. State and local agencies may also have information available about past floods. Basic guidelines are presented in "Flood Hazard Evaluation Guidelines for Federal Executive Agencies" [54]. These guidelines point out that there are three types of flood areas where flooding can be hazardous. First are riverine flood plains where floods are due to heavy rainfall or snowmelt runoff or to obstruction of a narrow channel. Second are coastal flood plains bordering on a body of standing water where floods can result from high tides, wind-driven waves, tsunamis (large waves caused by undersea earthquakes) or from a combination of these effects. Finally, debris cones, deposited at the base of a mountain by mountain streams, are subject to flash flooding. If it appears that the ADP facility is located in any of these areas, one must give consideration to flood exposure.

In evaluating the exposure to natural flooding, the ADP security planner should first examine the rules and regulations issued by his agency under Executive Order 11296. Next he should examine such evaluations of flood hazard as may be available for his own building or other nearby Federal buildings. These should help to determine the need to look more closely at the exposure. The information available will often allow the ADP security planner to estimate the probability of flooding to several levels. By examining the building layout, he can then estimate the probable effect on operations from damage or destruction of contents, interruption of electric power and communications, lack of access to the building, and the like. By relating these effects to the risk analysis, he will be able to estimate flood-related losses as a basis for cost justification of flood protection measures.

In addition to the overall effect of natural flooding, one should examine the flood damage potential from all causes. The first step is to evaluate the location of the ADP facility within the building. The basement is potentially the least desirable location since surface water from heavy rain or fire fighting water may collect in the basement. Drains can be equipped with backwater or check valves to prevent back up. Electrically driven sump pumps and ejector pumps may be provided to augment gravity drainage. However, in an emergency situation these may all prove ineffective. During a fire on an upper floor, the pumps and drains may be overwhelmed since fire fighting hose streams can easily pump a thousand or more gallons of water per minute into the building. Furthermore, it is possible that debris from the fire area may clog drains and pumps. Electric power for sump pump motors may be interrupted by a fire or hurricane—putting them out of service just when they are most needed. The ADP security planner should attempt to balance the physical protection offered by a basement location against the exposure to flooding and make a judgment about the net exposure. If the ADP facility is located in the basement and the flooding exposure is significant, it may be prudent to consider these countermeasures:

- **Sump pumps** (one or more) driven by gasoline motors for emergency use.
- **Drains** equipped with check valves.
- If surface water flooding is a significant threat, a supply of **sandbags** can be kept on hand to be used to construct a dike quickly. Heavy duty adhesive tape may be adequate to seal low lying exterior doors.
- It may be possible to install **masonry curbs** around the ADP area to divert flood water. This will help only with minor flooding but may be worth the effort.

These measures will be helpful where the exposure is modest or comes primarily from internal sources. For existing facilities having a significant exposure to external flooding, full scale flood proofing may be required. Excellent guidance will be found in "Flood-Proofing Regulations" [51]. This document is in the form of a model building code and provides guidance for minimizing flood-related hazards of building occupancy and for protecting structures against flood damage.

Flooding may also result from plumbing leaks. As a part of the threat evaluation, the ceiling above the ADP facility should be inspected for plumbing lines and for holes. Ideally no pipes should be routed over ADP hardware areas; where this is unavoidable, easily accessible shut-off valves should be provided. Likewise, chilled or condenser water pipes which suport air conditioning units inside the ADP area should have shut-off valves which can be used to isolate a leak. Major water lines should be instrumented to detect abrupt loss of pressure—a sign of catastrophic failure—to alert the building engineer and, perhaps, shut off pumps automatically so as to limit the amount of water which can escape. All holes in the floor slab over the ADP facility should be plugged with cement or similar material. Many buildings include so called wet columns. These are structural columns with adjacent vertical plumbing lines usually referred to as risers. As a rule one can identify a wet column because the walls enclosing it will be larger than most columns to allow space for the pipes. Since wet columns represent an increased exposure to leaks or flooding it would be preferable to exclude them from ADP areas. When this is unavoidable, each column should be checked to insure that any leakage will drain freely to the floor below.

Almost all computer rooms are equipped with a raised floor to provide a protected space for inter-cabinet and power cables (and often as a supply air plenum for the air conditioning system). If water collects under the raised floor, there is a danger that these cables will be affected. Inter-cabinet cables with connectors at the ends only should be highly water resistant. However, power cables often plug into receptacles located on the floor, risking short circuiting and corrosion. Where possible, receptacle boxes should be raised up from the floor at least eight to ten cm. and the wiring enclosed in unbroken rigid conduit. It is also desirable to provide positive water drainage with floor drains spaced about six meters apart. This is particularly important in new construction where the floor slab under the raised floor has been depressed to bring the raised floor flush with the surrounding floor. This eliminates the need for ramps but, without positive drainage in the depressed slab area, it is obvious that substantial amounts of water could collect under the raised floor. Not only would cables be submerged but each inch of water will add about five pounds per square foot to the live load, leading in extreme cases to structural damage or collapse.

An increasing number of ADP facilities are now stockpiling plastic sheeting to protect ADP hardware in an emergency. Several cases have been reported where the prompt use of such sheeting has protected hardware against leakage from broken plumbing or fire fighting on upper floors. Because of the modest cost and assured effectiveness of this countermeasure, it can be recommended highly.

2.3. Earthquake

Earthquakes represent a threat to ADP operations for two reasons. First, an earthquake may cause structural damage or collapse of the ADP facility building, interruption of electric or communications circuits, loss of utilities and other direct effects. Second are the more widespread effects on the community: disruption of transportation, food supplies and other vital services. As a result, many of the ADP staff may be unable to report for work and supporting services may not be available.

Assessing the probability of an earthquake is not easy because of the relatively short recorded history of earthquakes in the United States. Figure 2 shows the number and intensity of known earthquakes and figure 3 is a seismic risk map based on these data. Note that the latter map merely indicates the probable severity, not probability of occurrence. Ongoing Federally-sponsored research is expected to lead to the ability to forecast long term probability and possibly even actual occurrence. However, until such techniques become available it seems prudent for ADP facilities located in Zone 3 regions to assume that an earthquake which could disrupt operations for at least a week will occur at 50 to 100 year intervals. Furthermore, ADP facilities within about five to ten miles of major faults should probably assume total destruction of the facility with about the same probability of occurrence.

There are two types of potential countermeasures. The first is to select a building with high resistance to earthquake damage and so located as to be protected against damage from neighboring buildings. Locations which should be avoided include hillsides, land fill areas, waterfront areas, fuel storage areas, tall structures (such as buildings, radio towers or transmission lines) which might fall on the ADP facility or underground fuel transmission lines. One should bear in mind that the majority of the damage from the San Francisco earthquake was caused by the subsequent conflagration which raged uncontrolled from the lack of fire fighting water. For this reason consideration should be given to using sway bracing, flexible joints, etc. to make the sprinkler system earthquake resistant and to provide a reliable on-site water supply.

Beyond preventive measures such as these, the ADP security planner may wish to safeguard the agency mission by including off-site operation in the ADP facility contingency plan. In this case he must be careful to select locations which are sufficiently separated so as not to be affected by the same earthquake. Consideration should also be given to the location and construction of the facility used to store back-up files, documentation and the like in order to assure that these materials will be undamaged and accessible following an earthquake. Valuable guidance in risk analysis and remedial measures will be found in "Building Practices for Disaster Mitigation" [59].

2.4. Windstorms

Windstorms, hurricanes and tornadoes all represent potential threats to an ADP facility. Hurricanes are characterized by high winds and heavy rain resulting in structural damage, flooding and in many cases loss of electric power. Of 148 major electric power interruptions in the United States reported during the period 1954 to 1966, 17 were attributed to hurricanes—an average of 1.3 per year. In 1970, Hurricane Celia was reported to have affected some 50 data processing facilities (some quite seriously) in the Corpus Christi area. Power was off for as much as 36 hours.

A study of hurricane frequencies based on occurrences during the period 1886–1970, reported in "Atlantic Hurricane Frequencies Along the U.S. Coastline" [48], will be helpful to the ADP security planner in evaluating the exposure of his facility. Results of the study for high probability areas are summarized below:

Annual Probability (Percent)	Locations
16	Fort Lauderdale, Florida
15	Palm Beach, Florida
14	Brazoria County, Texas
13	Lafourche Parish, Louisiana
13	Mobile, Alabama-Pensacola, Fla.
13	Key West, Florida
12	Chambers County, Texas
11	Carteret County, North Carolina
9	Matagorda County, Texas
9	Franklin Parish, Louisiana
9	St. Bernard Parish, Louisiana

BEST COPY AVAILABLE

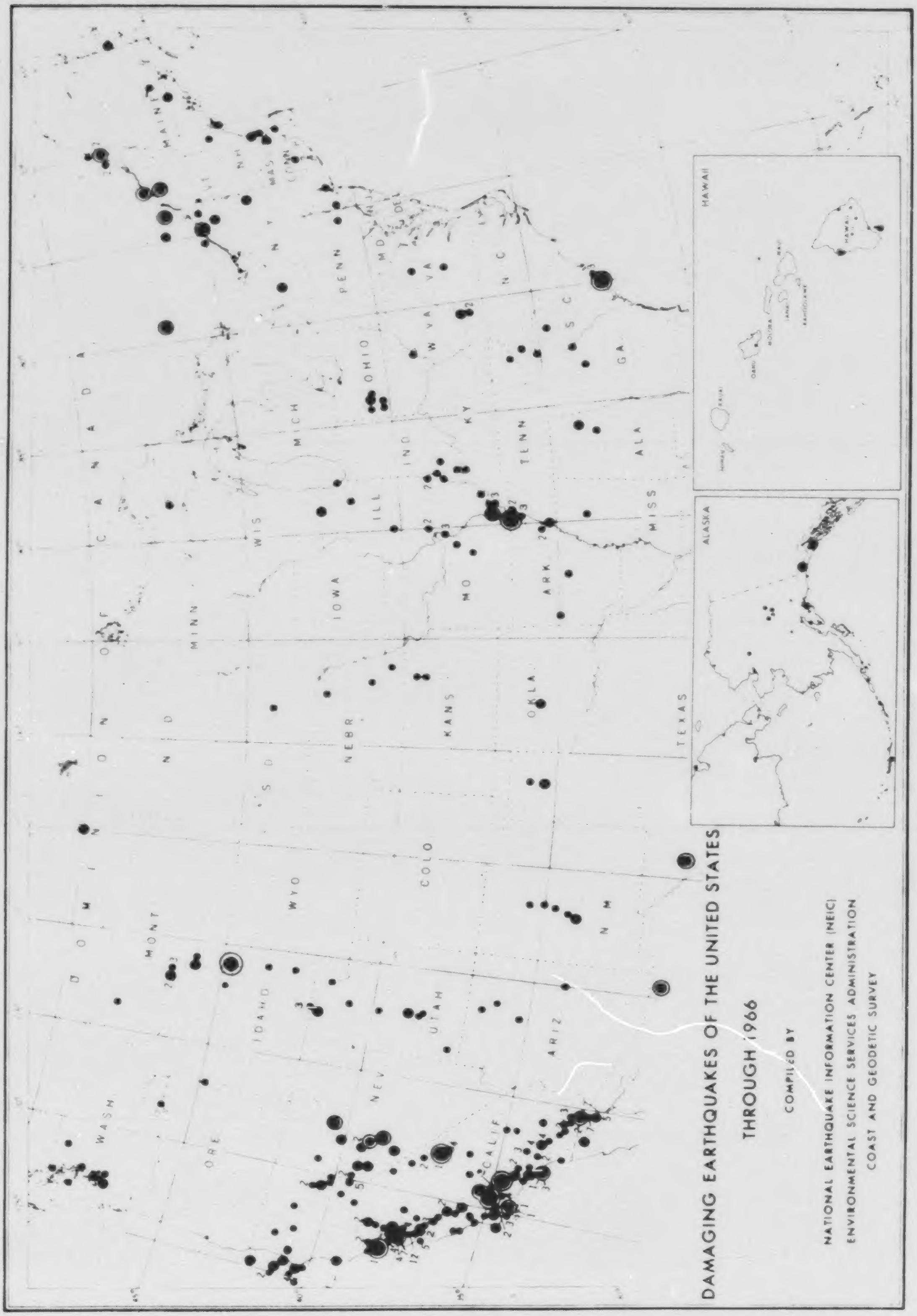
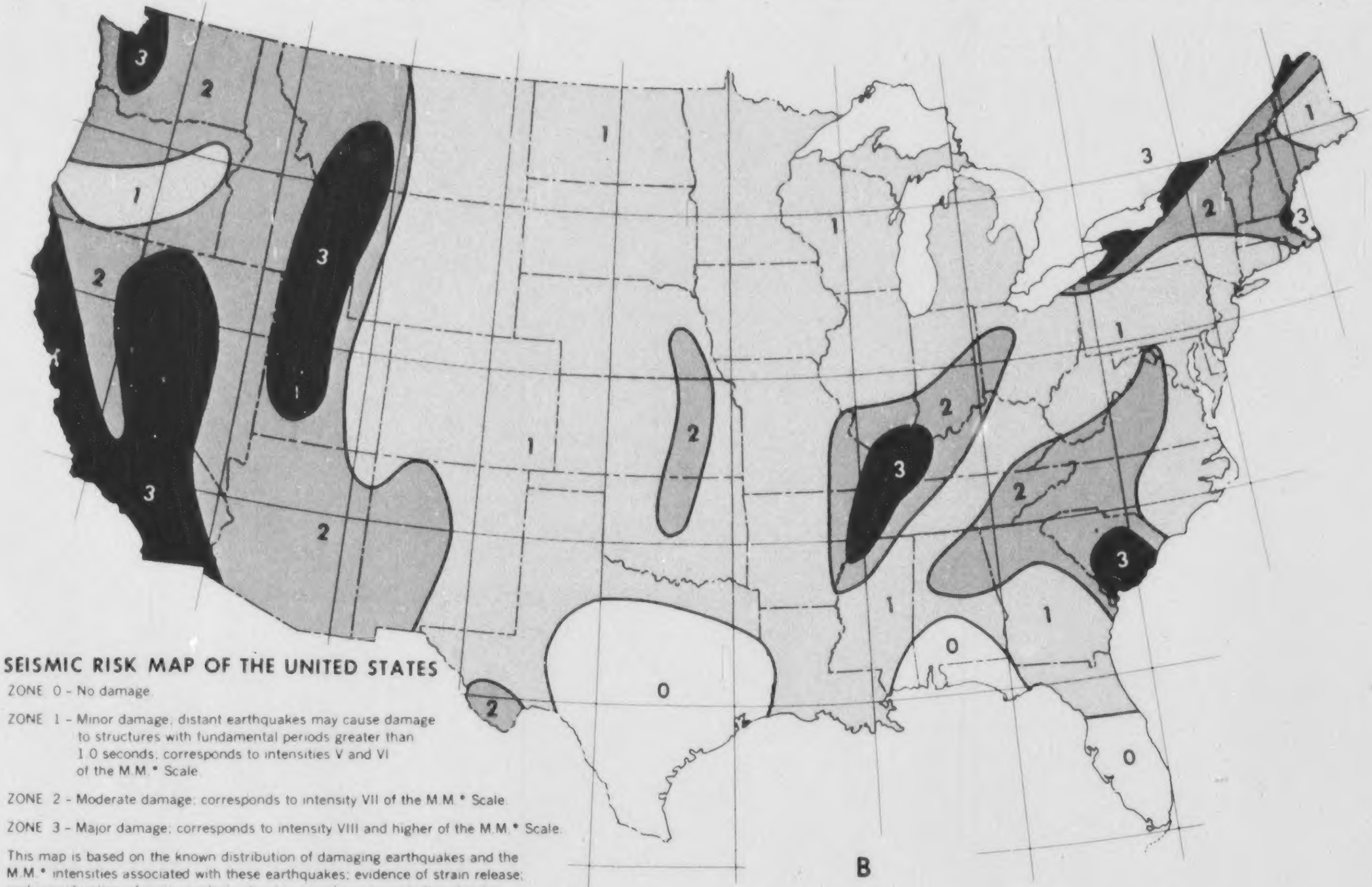

DAMAGING EARTHQUAKES OF THE UNITED STATES THROUGH 1966
COMPILED BY
NATIONAL EARTHQUAKE INFORMATION CENTER (NEIC)
ENVIRONMENTAL SCIENCE SERVICES ADMINISTRATION
COAST AND GEODETIC SURVEY
DOMINION OF CANADA
WASH
ORE
CALIF
NEV
IDAHO
MONT
WYO
UTAH
ARIZ
COLO
N M
N D
S D
NEBR
KANS
OKLA
TEXAS
MINN
IOWA
MO
ARK
WIS
ILL
MISS
MICH
IND
KY
TENN
ALA
OHIO
W VA
VA
N C
S C
GA
PENN
N Y
MD
DEL
N J
MASS
CONN
N H
VT
MAINE
ALASKA
HAWAII

FIGURE 2. *Damaging earthquakes of the United States through 1966.*

BEST COPY AVAILABLE



SEISMIC RISK MAP OF THE UNITED STATES

ZONE 0 - No damage.

ZONE 1 - Minor damage; distant earthquakes may cause damage to structures with fundamental periods greater than 1.0 seconds; corresponds to intensities V and VI of the M.M.* Scale.

ZONE 2 - Moderate damage; corresponds to intensity VII of the M.M.* Scale.

ZONE 3 - Major damage; corresponds to intensity VIII and higher of the M.M.* Scale.

This map is based on the known distribution of damaging earthquakes and the M.M.* intensities associated with these earthquakes; evidence of strain release; and consideration of major geologic structures and provinces believed to be associated with earthquake activity. The probable frequency of occurrence of damaging earthquakes in each zone was not considered in assigning ratings to the various zones.

*Modified Mercalli Intensity Scale of 1931.

Seismic risk maps. Because of the relatively short recorded history of seismic events in the United States, such maps can give only a rough idea of the long-term hazard. The maps are based on the actual occurrence of earthquakes and major geologic structures and provinces, but do not consider local physical conditions. No common time-scale is implied; actually, major earthquake damage would not be expected to occur as frequently in an East Coast Zone 3 as in a West Coast Zone 3. (A) Map compiled in 1948–1952, and incorporated into many building codes and regulations. The dots represent past occurrences of damaging earthquakes, and are defined as follows: smallest dots, negligible damage to buildings of good design; next smallest, slight damage to buildings of good design; second largest, considerable damage to buildings of good design; largest dots, great damage, fissures, visible vertical and horizontal ground movements. (B) Map released in 1969, based on additional seismic studies. (ESSA/USC&GS)

FIGURE 3. *Seismic Risk Map of the United States.*

BEST COPY AVAILABLE

Other localities on the Gulf and Florida coasts have probabilities in the range of 4% to 8%. The probabilities for Atlantic coast areas not listed above range from 7% to zero. If the ADP facility is in or near the high probability localities, the ADP security planner should give careful consideration to the threat from hurricanes.

Apart from measures to protect against flooding and electric power failure, described elsewhere in these guidelines, one should consider the resistance of the ADP facility building to wind damage, particularly windows broken by wind-driven debris or damage from falling trees, utility poles and the like. A "walk-around" inspection of the building should be adequate to identify potential trouble spots. Since ample warning is usually available, thought should be given to stockpiling plywood or similar materials for temporary protection of exposed windows and doors.

The occurrence of tornadoes by state during the period 1953 to 1969 is depicted in figure 4. There was an average of 642 tornadoes per year. The mean number per 10,000 square miles per year is tabulated below for the high incidence states:

State	Tornadoes/ 10,000 Sq. Mi./Year
Oklahoma	8.5
Kansas	6.0
Indiana	6.0
Massachusetts	5.4
Florida.	4.9
Iowa	4.5
Nebraska	4.3
Missouri	4.3

For all other states the incidence is less than four. There is some evidence to suggest that tornadoes tend to reoccur in some relatively limited areas. Therefore one should not base an estimate of occurrence probability on the gross figures given above. Rather, if the ADP facility is located east of the Rocky Mountains, the ADP security planner should consult with local authorities of the nearest National Weather Service office for information about the past record for the location of the ADP facility.

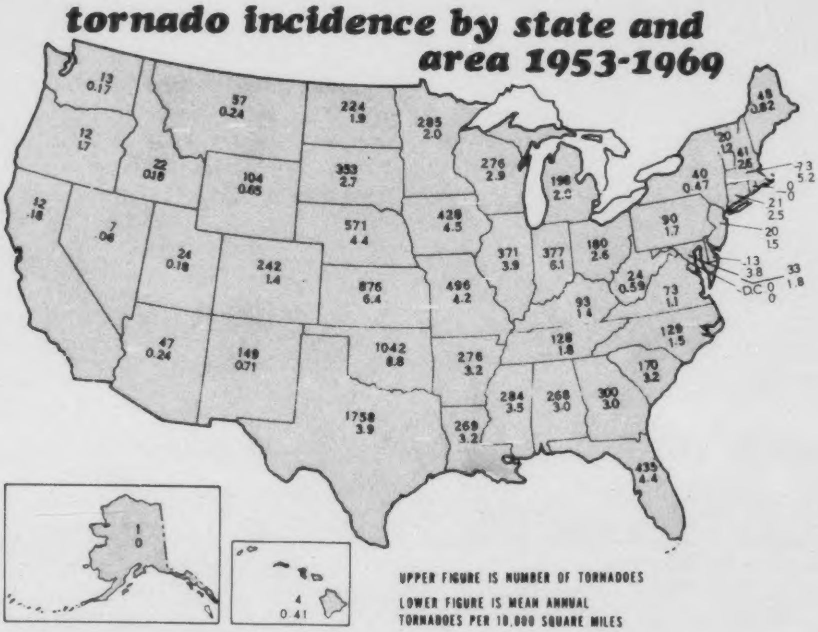

tornado incidence by state and area 1953-1969
13 0.17
12 1.7
12 .18
22 0.18
7 .06
57 0.24
104 0.65
24 0.18
47 0.24
242 1.4
149 0.71
224 1.9
353 2.7
571 4.4
876 6.4
1042 8.8
1758 3.9
285 2.0
428 4.5
496 4.2
276 3.2
269 3.2
276 2.9
198 2.0
371 3.9
377 6.1
180 2.6
93 1.4
128 1.8
284 3.5
268 3.0
300 3.0
435 4.4
170 3.2
129 1.5
73 1.1
24 0.59
90 1.7
40 0.47
20 1.2
41 2.6
48 0.82
73 5.2
0 0
21 2.5
20 1.5
13 3.8
33 1.8
D.C 0 0
1 0
4 0.41
UPPER FIGURE IS NUMBER OF TORNADOES
LOWER FIGURE IS MEAN ANNUAL TORNADOES PER 10,000 SQUARE MILES

FIGURE 4. *Tornado incidence by State (1953-1969).*

During a recent tornado in Georgia a water main above the computer room of a data processing facility ruptured and caused extensive flooding and the building evidently was badly damaged. Rapid reconstruction of the computer room in a nearby company building and hard work by the ADP staff and vendor engineers were major factors in rapid recovery. An effective data base management system and centralized administration of it, were also important factors. Some work was performed at off-site facilities and a week later work was back to the normal schedule at the temporary location.

Even if there is no damage to the building itself, an ADP facility may lose electric power because of a nearby tornado. During 1954 to 1967 there were ten major electric power interruptions reported to be caused by tornadoes and seven more to be caused by high wind.

To summarize, historic data should give a good indication of the probability of occurrence of hurricanes, tornadoes and high winds. Where the probability warrants the effort, the ADP security planner should give attention to measures to protect against building damage, flooding and electric power failure and should see that the contingency plan has the capability to meet such situations satisfactorily.

3. Supporting Utilities

3.0. Introduction

Every ADP facility is dependent on supporting utilities: electric power, air conditioning and often others such as communications circuits, water supplies and elevators for its operation. The ADP security planner should consider the probability of occurrence and the effect of breakdowns, sabotage, vandalism and such accidents as fire, flooding and the like on these utilities. He can then relate the effects to the needs of the ADP facility as established by the risk analysis. This chapter discusses the factors affecting such events and measures to guard against them.

3.1. Electric Power

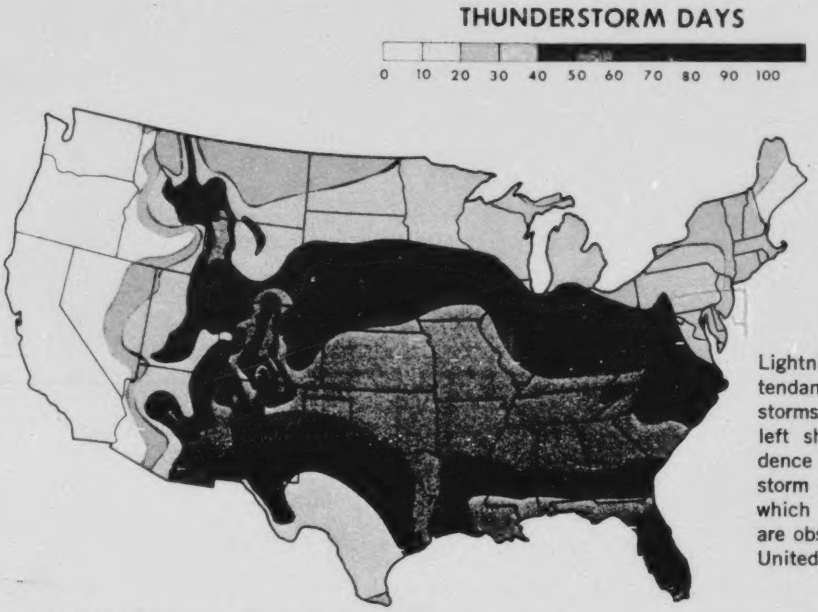
Electric power as it affects ADP operations has two significant characteristics: quality and reliability. Quality is used here to refer to the absence of variations from the normal waveform which are too small to be recorded by the local electric utility company but, depending on the ADP hardware, are large enough to affect operation of ADP hardware. Typically the ADP hardware rectifies the alternating electricity, filters and voltage-regulates the resulting direct current and applies it to the ADP circuitry. The filtering and regulation cannot be expected to eliminate voltage variations beyond a reasonable range. If line voltage is 90% or less of nominal for more than four milliseconds, or 120% or more of nominal for more than 16 milliseconds, one can expect excessive fluctuations in the DC voltage applied to the hardware circuitry. The effect on the circuitry is difficult to predict since it will depend on the amount and duration of the fluctuation and the state of the hardware. One may expect to find logic errors, erroneous data transfers or, in extreme cases, damage to hardware. Such things are usually obvious immediately, while other effects can go unnoticed until much later, if ever.

These power line fluctuations, usually referred to as transients, can be caused by lightning strikes. Their probability of occurrence is dependent on the number of thunderstorms, the spacing between substations and the use of underground, as opposed to overhead, distribution lines. Figure 5 shows the incidence of thunderstorm days in the United States. Experience has shown that there will be approximately one lightning induced transient at an ADP facility for every three thunderstorm days, with a somewhat higher rate in rural areas and about one third as many in urban areas where distribution lines are underground.

Utility company transients are more difficult to predict but it is not unusual to find a transient every morning at about 7:30 a.m. when energy demand begins to build up and power factor correcting equipment is switched offline. As a rule, such transients will not affect ADP operations, but cases have been reported where major problems were experienced every morning.

Internally generated transients will depend on the configuration of power distribution inside the building and the percentage of total load represented by the largest single switching load. The effects of internal transients can be minimized by isolating the ADP hardware from other building loads. Ideally the computer area power distribution panels should be connected directly to the primary feeders and should not share step-down transformers with other loads, particularly high horsepower mo-

BEST COPY AVAILABLE



Lightning is the attendant of thunderstorms. The map at left shows the incidence of thunderstorm days—days on which thunderstorms are observed—for the United States.

Alaska and Hawaii are less than 10.

FIGURE 5. *Thunderstorm days.*

tors. A typical power distribution system is shown in figure 12.

This discussion has outlined the causes and effects of power line transients, but it is difficult to develop good estimates for frequency of occurrence from abstract considerations. Fortunately, equipment is available which enables one to measure the actual occurrence of transients. Typically the device will include a strip chart recorder and electronic circuitry which will cause even brief or minor transients to be permanently recorded. By comparing the times when transients occurred with the console log records of abnormal operation one can usually determine the number of disruptive transients in a given time period and often the cause of the transient. Such measurements should be made for at least a month and some ADP facilities do so continuously. However, there are two pitfalls. First galvanometer recorders will not respond to brief transients and so display only the line voltage trend. For this reason they will not be helpful in dealing with transients. Second it is important to see that a qualified electrical engineer supervises measurements closely. If the measurements are to be useful, they must be carefully made, intelligently interpreted and correlated with other inputs. Discussions with representatives of the local electric utility will also be helpful in understanding the causes of observed transients.

The second basic quality of electric power—reliability—has to do with the number and duration of occasions when the line voltage departs from nominal for periods too long to be considered transients. One may observe sustained undervoltage (brownout) or actual failure (blackout). Brownouts are a result of load near to or equalling generating capacity. In extreme cases the public utility will deliberately reduce line voltage by a maximum of 8% to stretch the generating capacity to meet demands. As a last resort they may actually disconnect a portion of the load, a procedure referred to as "load shedding," but which, for affected customers, is a blackout. In addition, blackouts may result from windstorms, floods and similar causes noted in Chapter 2, from failures of electric system equipment or, in rare cases, from human error.

The famous Northeast blackout of 1965 revealed basic defects in the systems and procedures for power pool management. Hopefully, the measures since taken to increase the reliability of the national electric system make a repetition unlikely. Nonetheless, certain problems remain, e.g., the inherent reliability of generating equipment, particularly very large units; and new probems are arising, e.g., environmental protection measures, which make new construction to meet growing demand a lengthy process. The probability of occurrence of a blackout will depend on both random failures at a more or less constant rate and the need for load shedding which depends on the amount of reserve generating capacity. Each factor must be evaluated separately.

During the first half of 1967, fifty-two significant random power failures in the United States were reported by the Federal Power Commission (FPC) [10]. It seems reasonable to assume that this is a representative sample and that similar failures will occur at the same rate in the future. Less widespread or less significant events are not centrally reported —events such as transformer breakdowns, local accidents severing electric lines and other mishaps. There is no way to predict the frequency or imminence of these random or near-random events.

The same FPC report suggests that the duration of randomly caused blackouts is about as follows:

Duration	Percent of Total	Cumulative Total
9 - 15 minutes	6%	6%
15 - 30 minutes	36%	42%
30 - 60 minutes	18%	60%
1 - 2 hours	14%	74%
2 - 4 hours	10%	84%
4 - 8 hours	8%	92%
8 - 16 hours	6%	98%
16 or more hours	2%	100%

The probability of loss of service due to blackouts or load-shedding by the local utility can be foreseen to some extent by becoming familiar with its generating capacity, its reserves and, possibly, its current reliability and maintenance situation. If the reserve capacity is 20% of peak load, the probability of load related blackout is very small. As reserve capacity approaches the capacity of the largest single generating unit, the probability of a blackout rises rapidly and an even lower reserve capacity represents a precarious situation. Current information in this and related areas can be obtained from FPC reports and the National Electric Reliability Council [22].

By considering all these factors, one can estimate the effect of power transients and failures with some confidence. By referring back to the risk analysis, he can then estimate the cost of these transients and blackouts to the ADP facility. This cost estimate is then used to cost-justify protective measures. Of course, one should be careful to take into consideration projected growth in particularly sensitive applications such as real-time or teleprocessing in projecting future loss potential.

With a reasonable estimate of potential losses, the ADP security planner is in a position to evaluate candidate countermeasures on a cost-performance basis. There are a number of possible measures which address one or more quality problems at a range of costs. In the discussion which follows, general price ranges are included and will be stated in terms of kilovoltamperes (KVA) of load. While these prices will be helpful for preliminary analysis, they should be used with caution and final decisions should be based on accurate estimates.

As a part of the analysis of protective measures, the ADP security planner should obtain an accurate tabulation of these types of loads: the ADP hardware including data transmission devices, data conversion equipment, air conditioning equipment, normal and minimal lighting and other equipment essential to emergency operation such as boilers, power doors, etc. He should make a "one-line" diagram of the electric power distribution arrangement for the building, particularly for the loads given above, down to the individual breaker panel level. These data are necessary to evaluate possible remedial measures to be described.

If the major loss is expected to come from internally generated transients, a rearrangement of the power distribution may effectively solve the problem. No useful cost guidance can be given since it will depend on the particulars of the specific situation.

In some cases it may be economically feasible to connect the building to more than one utility feeder via transfer switch. Thus if one feeder fails, the building load (or by splitting the main bus bar only critical loads) may be transferred to the alternate feeder. This technique is of greater value if the two feeders connect to different substations. Since dual feeders only protect against localized blackouts, they are of limited value but one may in some situations find the cost justifiable.

A voltage regulating transformer (VRT) will provide significant protection against minor long-duration transients (4 milliseconds or more) and brownouts at a cost of about $100 to $200 per KVA of load. However, VRT's will not protect against brief, high-intensity transients or actual power failures.

At a cost of $200 to $300 per KVA, one can install a motor-alternator (motor-generator) set which includes an energy storage flywheel, as shown in figure 6. Such a configuration will protect very effectively against transients and power failures up to about 15 seconds in duration. While reliability is quite high, one must allow for regular maintenance, particularly of bearings. It will be necessary to provide a special room for the equipment because the acoustic noise level is quite high and the floor loading may be above normal.

A number of vendors now offer what are referred to as uninterruptable power supplies (UPS). The typical UPS consists of a solid state rectifier which keeps a battery charged and drives a solid state inverter. The inverter synthesizes alternating current for the computer. A simplified block diagram is given in figure 7.

In effect, the UPS simulates the motor-flywheel-generator set with the battery acting as a huge flywheel. Depending on the ampere-hour capacity of the battery, the UPS can support its load for as long as 45 minutes without input electricity. At the same time, it will filter out transients and compensate for brownouts. The cost for a UPS is in the range of $700 to $900 per KVA plus installation and site preparation costs, such as added air conditioning and floor reinforcement.

To provide extra capacity, to clear load faults and to protect against a failure of the UPS, one can insert a static transfer switch between the UPS and the computer loads as shown in figure 8. The control circuitry for the static switch can sense an over-current condition and switch the load to the prime power source without causing a noticeable transient.

When the total load exceeds 100 KVA or so, it may be economically feasible to use multiple, independent UPS units as shown in figure 9. Since each unit has its own disconnect switch, it can be switched off line should it fail for any reason.

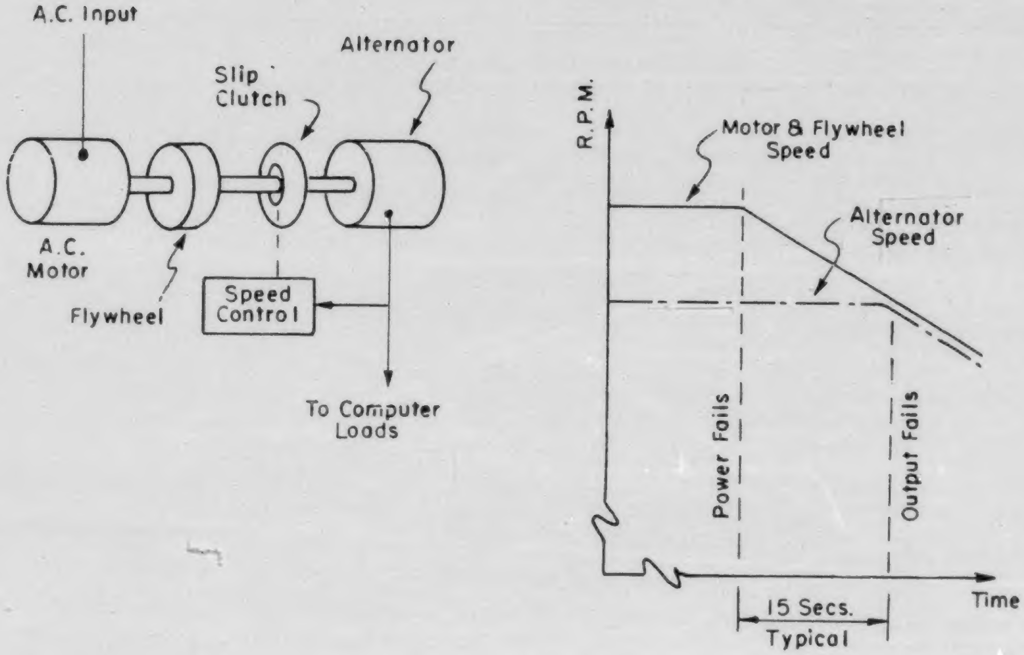


FIGURE 6. *Typical motor-alternator set with flywheel energy storage.*

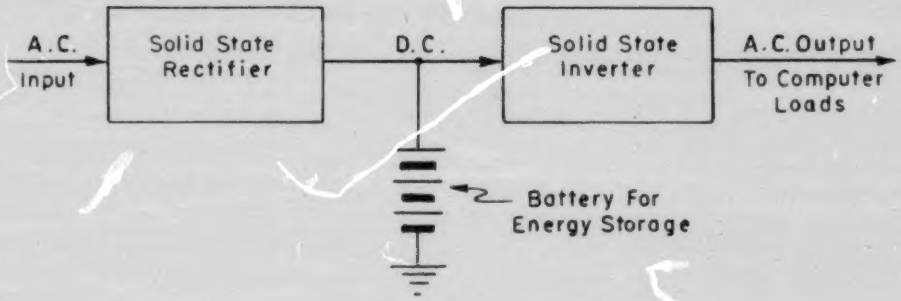

A.C.
Input
Solid State Rectifier
D.C.
Solid State Inverter
A.C. Output
To Computer Loads
Battery For Energy Storage

FIGURE 7. *Simplified block diagram of an uninterruptable power supply.*

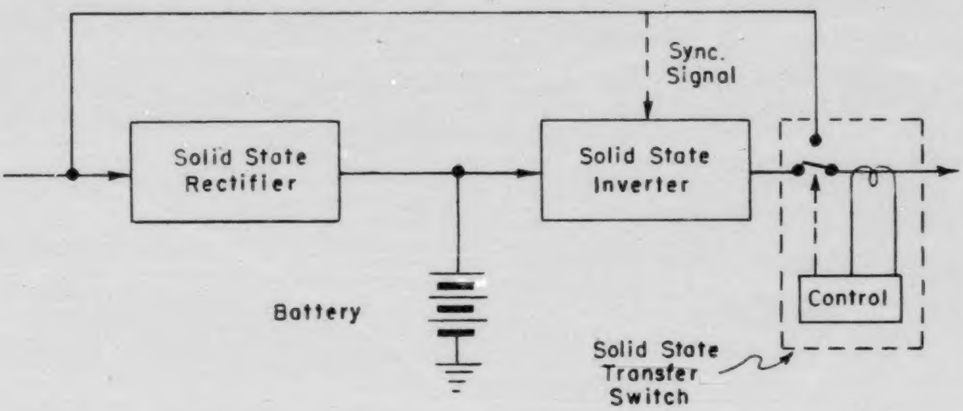

Sync. Signal
Solid State Rectifier
Solid State Inverter
Control
Battery
Solid State Transfer Switch

FIGURE 8. *UPS with transfer switch.*

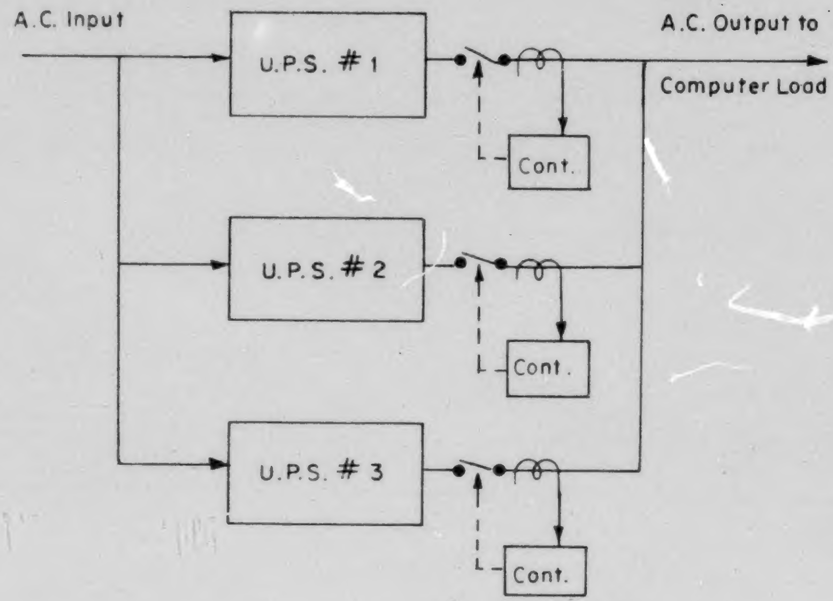


FIGURE 9. *Multiple independent UPS units.*

Finally, if the risks analysis has shown a major loss from power outages beyond 30 to 45 minutes, one can install on-site generation, as shown in figure 10 at a cost of about $100 per KVA plus installation and site preparation. The prime mover may be a diesel motor or a turbine. When the external power fails, the control unit starts the prime mover automatically which in turn brings the generator up to speed. At this point, the UPS switches over to the generator. Barring hardware failures, the system will support the connected load as long as there is fuel for the prime mover. Note that the generator must be large enough to support other essential loads such as air conditioning, minimum lighting, etc., as well as the UPS load.

There are many variations on the configurations shown here. If it appears that one or more of these measures can be cost justified, one should seek expert help in determining optimum performance specifications and the best overall solution to the problems of integration into the building power distribution before deciding on a particular configuration. Furthermore, one must remember that in addition to the rough cost guidelines given above, one must allow for any special installation costs, the cost of the floor space required for the equipment, the cost of any needed alterations to the air conditioning for the space, the cost for equipment maintenance and the cost of additional electric energy which will be dissipated by the equipment. Because of these complex cost factors, the analysis is a lengthy process. It is hoped that the discussion here will provide enough information to permit the ADP security planner to determine if a detailed analysis is warranted. A helpful discussion of UPS systems will be found in "Consultants Guide to Uninterrupable Power Supply Systems" [57].

In the event of a fire, flooding or other emergency, it is important to be able to shut off electric power quickly, easily and selectively. First, one can use the power-off switch on the individual unit. However, one should remember that the power cable and circuitry up to and including the built-in power-off switch are still energized. These can be de-energized by manually tripping the branch circuit breaker at the distribution panel. To do this easily and effectively, several conditions must be met. Distribution panels should be located in the computer room and access to them must be unobstructed. It is not uncommon to find distribution panels hidden by other equipment or otherwise difficult to reach. Individual circuit breakers must be clearly marked so that one can quickly and accurately determine which circuit breaker is associated with each hardware unit. Finaly, one can disconnect all power from computer room loads except for room lighting. While this can be accomplished by throwing the necessary disconnect switches, they may be located some distance from the computer room. To avoid this problem, RP-1 [9] requires that a master control switch be located near the console and just inside each principal entrance to the computer room which, when depressed, will disconnect power to all electronic equipment. NFPA Standard No. 75 [34] requires that power to ventilating equipment be disconnected as well, but it is suggested that this not be done without first considering the factors given in section 3.2.

While these master control switches perform a vital emergency function, it is obvious that their inadvertent operation will be extremely disruptive. For this reason it is important to see that they are clearly marked as to function and physically designed to require deliberate effort to operate them. Figure 11. shows one solution to this problem. The master control switch shown in the figure is inside a plastic box located about six feet (2.0 m) above floor level. Accidental or careless operation appears to be highly unlikely.

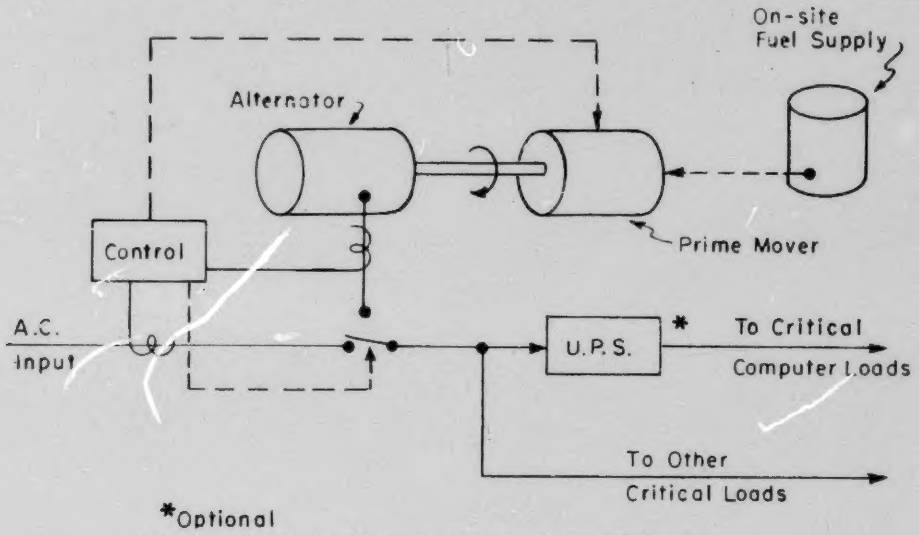


FIGURE 10. *UPS with on-site generation.*

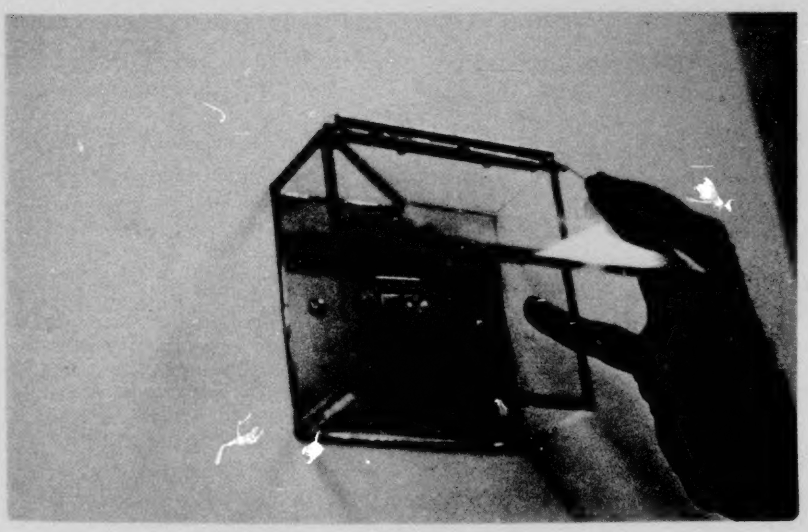


FIGURE 11. *Plastic box to protect master control switch against inadvertent operation.*
Photograph courtesy of Shell Oil Company

A one-line diagram of a typical building power distribution system is shown in figure 12 to clarify the preceding discussion. Beginning at the top, we see that power flows through a series of step down transformers, disconnect switches and overcurrent protective devices (fuses) until it reaches the individual distribution panels. Each panel has a number of circuit-breaker protected branch circuits to which individual hardware units are connected. This basic configuration can be modified in a number of ways to enhance quality or reliability. First one could take pains to isolate ADP circuits from equipment which generate transients, e.g., high horsepower motors. The greater the distance from the ADP facility to the substation, the greater the probability of a feeder failure, all other things being equal. If feeder failure appears to be a signicant threat, one can usually arrange for a second feeder (ideally from a different substation) to be run to the ADP facility. A transfer switch which can be either manual or automatic is used to switch the step down transformer from the primary feeder to the back-up feeder in the event of a failure. Alternatively, one might isolate critical building loads, e.g., ADP bus bar, ADP air conditioning, emergency lighting, security hardware, and supply them through a completely separate power distribution system. In this case only the critical load need be switched to the back-up feeder. This arrangement insures isolation, and the cost of the back-up feeder is reduced since it does not have to carry the entire building load. This may have a major impact on the cost justification.

With the help of the building manager or engineering staff, the ADP security planner should check these points about the power distribution system:

(a) Electric wiring conforms to the requirements of the National Electric Code [55], NFPA No. 75 [34] and RP-1 [9].

(b) Procedures are established in coordination with the building manager to insure that electrical maintenance work is coordinated with ADP operations to avoid inadvertent shut-off of computer room, air conditioning or communications power. It may be desirable to label sensitive disconnect switches "up stream" of the computer room, but not in such a way as to flag them for a saboteur.

(c) All electric power distribution equipment is adequately protected physically against accidental damage or sabotage. Protection may include such things as control over access to electrical equipment rooms and closets, barriers to protect utility poles and exterior transformer pads against damage by vehicles and avoidance of proximity to fire hazards.

In summary, the appropriate steps should be taken to assure that the quality and reliability of electric power will satisfy the needs of the ADP facility. Depending on the risk analysis and cost factors these measures may include changes to the power distribution system configuration, dual feeders, devices to filter out transients, uninterruptable power supplies, devices to compensate for brownouts, on-site generators and physical protection against tampering, sabotage or accidents. In addition, the wiring should conform to applicable codes and be properly integrated with the fire safety program.

3.2 Air Conditioning

Properly conditioned computer room air is important for three reasons. First the electronic circuitry requires fairly close temperature limits to minimize erratic operation. High temperatures (above about 30°C) may cause permanent damage to ADP hardware. Second, humidity control is required to assure proper operation of tabulating card devices and tape drives. Excessive humidity may cause cards to swell and feed erratically. Very low humidity often leads to static electricity buildup which can affect tape handlers, line printers and sometimes the ADP hardware itself. Finally, it is important that the room air be free of contamination which may be corrosive, conductive or large enough to cause disk drive head-crashes.* To the extent that controls over temperature, humidity or contaminants fail, ADP operations may be hampered or hardware damaged. In extreme cases it may be necessary to suspend operations until the situation can be corrected. Furthermore, if the computer room is a part of a building-wide air conditioning system, smoke from a fire elsewhere in the building may be introduced into the computer room.

In order to properly assess the exposure to these potential hazards, the ADP security planner should review the air conditioning system for the ADP facility with the building manager. Figure 13 shows a typical air conditioning system in diagrammatic form. The heart of the system is the air handling unit (AHU) through which computer room air is circulated by a fan. The function of the AHU is to provide temperature and humidity control and air filtering. To refresh the room air, outside air is drawn in through a louver in an exterior wall and mixed with return air. In addition, there may be an exhaust fan as well.

---

* One type of humidifier operates by atomizing water and injecting it into the air stream. This type should not be used in hard water areas because minerals in the water will be deposited on the ADP hardware.

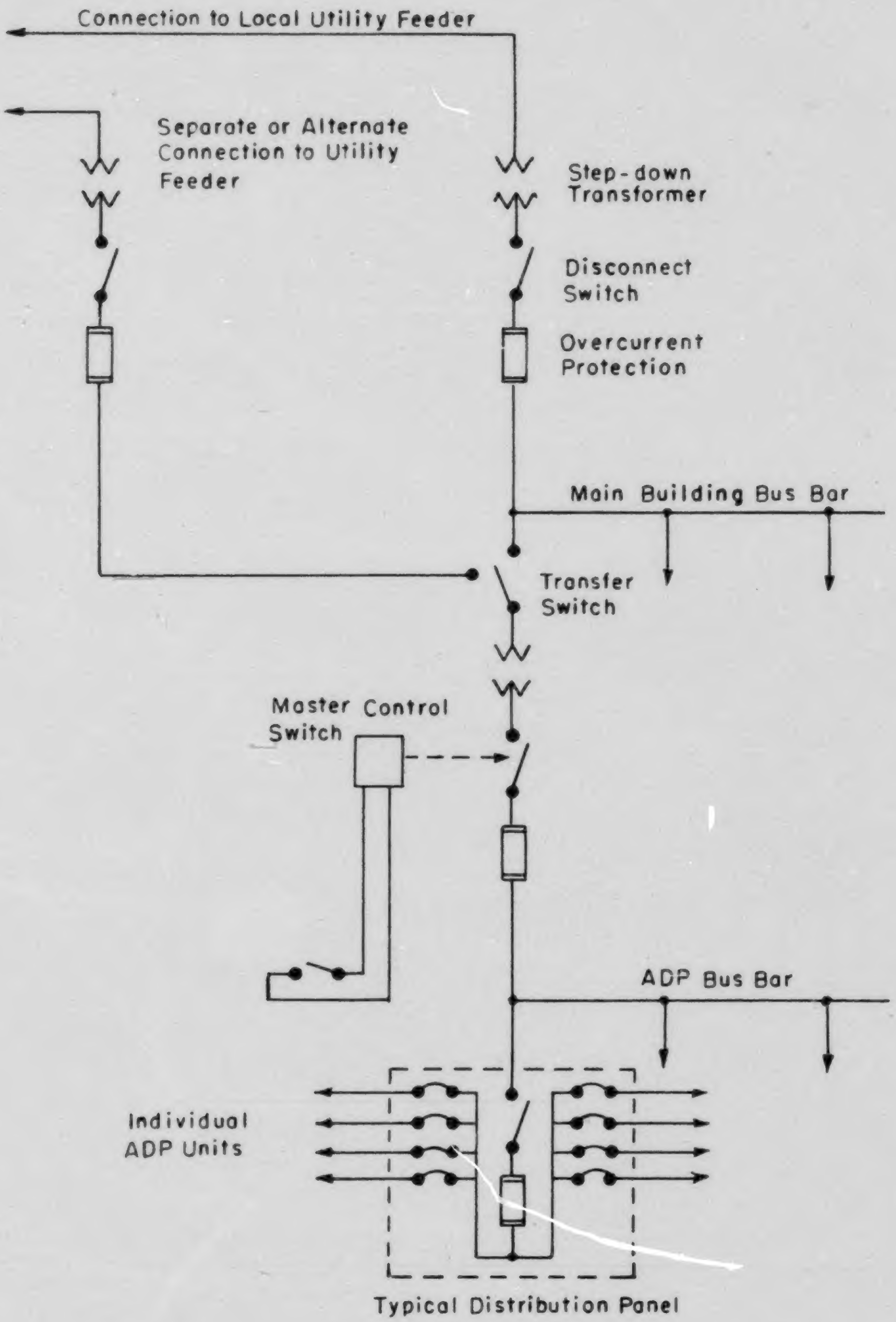

Connection to Local Utility Feeder
Separate or Alternate Connection to Utility Feeder
Step-down Transformer
Disconnect Switch
Overcurrent Protection
Main Building Bus Bar
Transfer Switch
Master Control Switch
ADP Bus Bar
Individual ADP Units
Typical Distribution Panel

FIGURE 12. *Simplified one-line diagram of power distribution.*

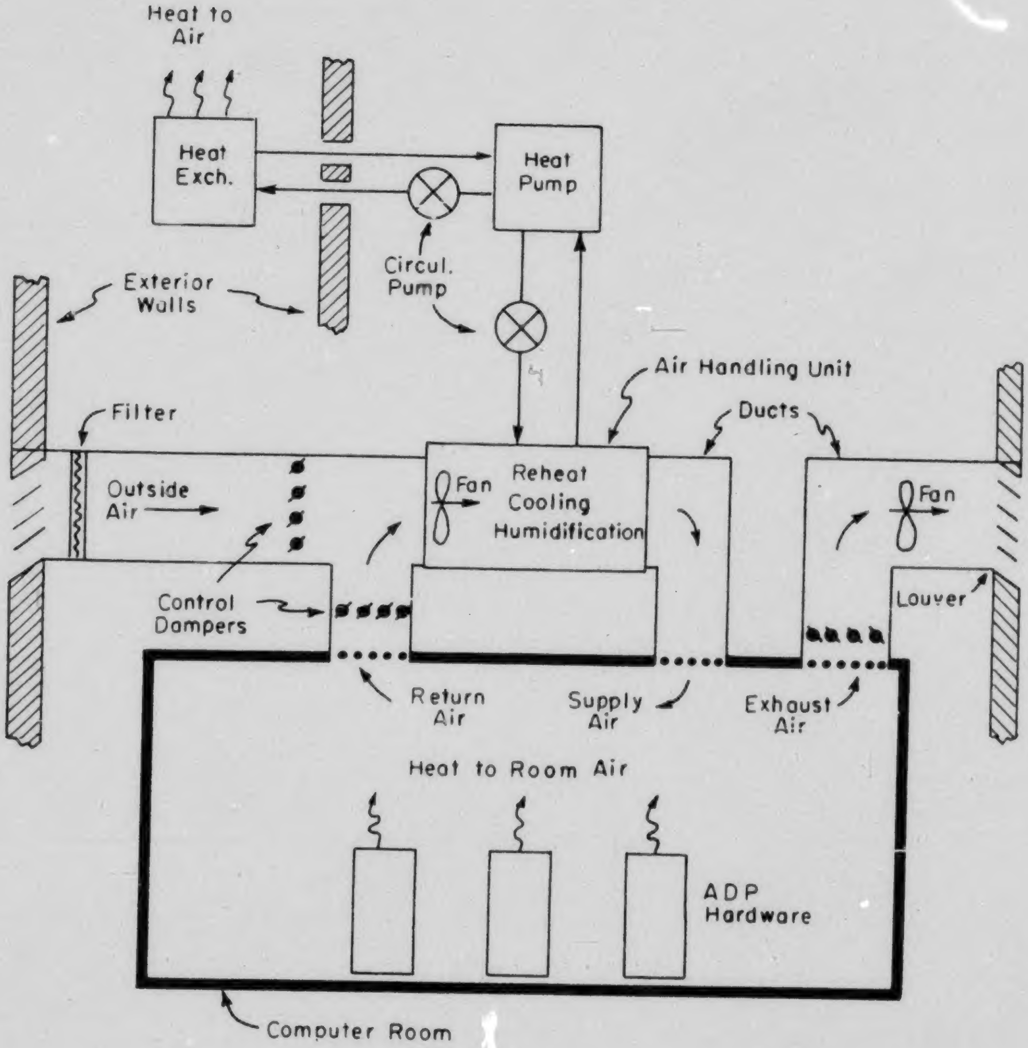

Heat to Air
Heat Exch.
Heat Pump
Circul. Pump
Exterior Walls
Air Handling Unit
Filter
Ducts
Outside Air
Fan
Reheat
Cooling
Humidification
Fan
Control Dampers
Louver
Return Air
Supply Air
Exhaust Air
Heat to Room Air
ADP Hardware
Computer Room

Figure 13. *Cross-sectional schematic diagram of a typical air conditioning system.*

Air flows through ducts, usually made of sheet metal, and proportioning is controlled by motorized dampers. To perform its function, the AHU needs a supply of water or steam for humidification during periods of low humidity, and some way to exhaust the heat removed from room air. This latter is done by connecting the AHU with some kind of heat pump (a chiller, direct expansion unit, etc.) by means of a refrigerant (e.g., chilled water) circulated by a pump. Likewise, the heat pump must have some means to dissipate the heat, usually a cooling tower or condenser.

The actual arrangement of system elements will depend on its size and local conditions. For example, a typical residential window air conditioning unit will combine all the functions except humidification into a single unit. Quite often computer rooms make use of so-called packaged air conditioning units which perform all functions except air intake and exhaust and heat exchange. In large buildings it is quite common to use one or a few heat pumps to support building comfort air conditioning as well as computer room AHU's. From this discussion one can see that there are many different devices which can fail with different consequences to ADP operations. The major failure modes, their effect and possible countermeasures are tabulated below in general terms.

Failure	Effect	Countermeasures
Outside air damper or fan.	**No outside air, but usually not critical.**	**Multiple outside air sources.**
AHU fan.	**No air circulation. Temperature rises.**	**Multiple AHU's.**
AHU humidity control.	**Loss of humidity control. Critical if outside air humidity is very high or low.**	**Multiple AHU's.**
AHU temperature control.	**Temperature rises.**	**Multiple AHU's.**
Circulating pumps, heat pump or heat exchanger.	**Temperature rises.**	**Multiple units interconnected so affected unit can be taken off line. Use outside air, and even floor fans, temporarily.**

To minimize the effects of failures, one can use multiple units, interconnected to permit affected units to be taken off line or to permit outside air to be used in an emergency. As an example, consider the situation where the computer room requires 50 tons of cooling, the balance of the building requires 100 tons for comfort air conditioning and a chilled water system is to be used. Two different system configurations are tabulated below:

Simple	Redundant
One 150 ton chiller	Three 50 ton chillers
One chilled water circulating pump	Three chilled water circulating pumps
One 50 ton computer room AHU	Three 20 ton computer room AHU's

While the simple system will meet the need, the failure of any single piece of equipment will probably require ADP operations to be halted within a few minutes to a half hour. The redundant system will be somewhat more expensive but failure of a given unit can be accommodated. If one or two chillers or circulating pumps fail, the computer room can still be supported by reducing or cutting off the comfort air conditioning to the balance of the building. If a computer room AHU fails, operations can probably be continued by reducing the heat load. This can be done by reducing lighting and turning off the least important ADP hardware.

Both as an emergency procedure and as normal energy conservation, outside air can be used for cooling if the temperature and humidity are low enough. How high the temperature of the outside air may be and still be effective for cooling depends on three things: the maximum allowable room-ambient or equipment intake temperature (either or both may be specified), the amount of heating that takes place in the air-handlers and ducts and the degree to which outside air (as opposed to recirculated warm air) may be used. Most of the existing air conditioning installations do not allow for an intake of only outside air, although in some cases it may be feasible and cost effective to modify the ducts and venting to permit this.

Assuming a 100% intake of outside air and exhaust of room air, there can be a temperature rise of up to 15 °F (8 °C) between the temperature at the intake to the air handling units and the warmest spot in the computer room. If, therefore, the maximum allowable temperature in the computer room is to be 90 °F (32 °C), then the highest temperature at which outside air may be used would be on the order of 75 °F (24 °C). However, this should be determined for each installation, based on its equipment specifications and air conditioning configuration.

In extreme emergencies it may be possible to use floor fans to exhaust computer room air to other parts of the building.

To evaluate the inherent system reliability, one should consider the factors already discussed, past failures and the estimated time to repair. This latter will depend on the availability of spare parts and qualified service personnel. The building engineering staff will be able to help with this estimate and with consideration of alternate means of increasing reliability. It is also desirable to keep one or more temperature-humidity recorders to monitor performance. Assuming normal operation, such records should be reviewed each week to discover erratic or inadequate performance, identify the cause and institute corrective action. One recorder should be kept in a fixed, central location to permit week-to-week comparisons. Additional fixed units may be desirable for computer rooms in excess of 1,000 square feet (100 m.²). Finally, if problems are encountered with even temperature distribution, it may be helpful to have an additional recorder for spot checking.

Since computer hardware is relatively sensitive to dirt and corrosion, the source and filtering of the outside air is important. When air intake louvers are located at ground level, there is a danger that excessive dust or dangerous fumes will be ingested. In one case a skunk near an air intake louver was disturbed by a maintenance worker who was cutting the grass. The resulting odor forced the total evacuation of a three story building! Further, it is important to see that filters are adequate and that they are inspected regularly and cleaned or replaced as needed.

Because the air conditioning system is used to move air within the building, it is important to be able to predict and control its operation during a fire. Referring to figure 13 one can see how the air conditioning system can be used to exhaust smoke from a computer room by closing the return air damper and fully opening the intake and exhaust dampers. Since prompt smoke removal will limit damage and permit fire fighting, such an arrangement is preferred to a complete shut down of air conditioning. However, if smoke will be forced into other parts of the building or ducts will be subjected to high temperatures, then shut-down is required and can be included as a part of the functions of the master control switch described in section 3.1.

Figure 14 shows a typical building air conditioning system. Return air and fresh air are mixed at the top floor of the building, passed through an AHU and then distributed to each floor of the building via the main supply duct. It can be seen that with such a system, smoke from a fire on the first floor would be quickly distributed throughout the building unless fire dampers were provided. Furthermore, the duct work may provide an avenue for the spread of a fire. In a recent ADP facility fire, air conditioning ducts were routed along the basement ceiling and then up through holes in the floor slab to a first floor computer room. When a fire started in packing materials stored in the basement, these ducts quickly failed and heat and flames entered the computer room. Extensive damage was done to hardware and supplies. For these reasons, air conditioning systems should conform to NFPA Standard No. 90A [28] as required by RP-1 [9]. Figure 14 illustrates a number of these requirements which can be briefly summarized as follows:

> Where ducts pass through fire walls they are equipped with automatically operating fire doors.
>
> Fire dampers are required at fire rated walls which are intended to restrict the spread of the fire, at openings in vertical shafts and other similar points.
>
> Smoke and heat detectors properly located in the duct work and emergency shut down controls are required to protect the system against smoke or high temperature air.

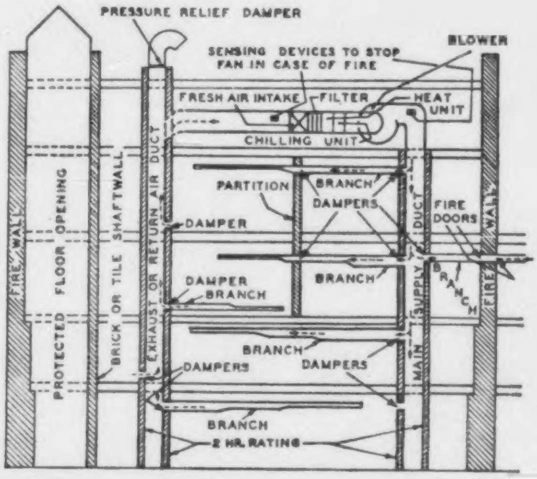


FIGURE 14. *Typical air conditioning system in a fire resistive building.*

NFPA Standard No. 90A [28] also requires that ducts, filters and other parts be noncombustible, that electrical wiring and equipment conform to the National Electric Code [55] and that in general the air conditioning system not defeat building features intended to limit the spread of a fire. The Standard also includes criteria for determining if the system can be used safely for smoke removal as has been suggested above for the computer room. The key factors are the ability of the system to handle high temperature gases and the effect on life safety objectives. In summary, it is important for the ADP security planner to understand the operation of the building air conditioning as it effects fire safety, and to identify the corrective actions needed to provide protection for the ADP facility. In section 3.1 it was asserted that emergency electric generating equipment should have enough capacity for minimum lighting and air conditioning as well as for the ADP equipment. It follows that the efficiency of the air conditioning system then effects not only its own cost of operation, but also the size and cost of emergency generators. The power required to operate ADP air conditioning is substantial, being on the order of 40% to 75% of the power required by the ADP equipment, lighting and other loads. This says that for every kilowatt of load removed in an emergency, the power input requirement is reduced by roughly one-and-one-half kilowatts.

Few ADP air conditioning systems were designed with energy costs and unavailability and the requirement for backup electric generators as significant design constraints. This may be one of the reasons it is quite common to find computer rooms operating at 72-75 °F (22-24 °C) and 50% RH and consequent dewpoints of 52-55 °F (11-13 °C), while the chilled water used for cooling may be supplied at 42 °F (6° C). Therefore, the chilling units are constantly extracting water from the air. Not only does this reduce the cooling efficiency and require considerably more energy, but even more energy will be required to add water back into the air to bring the relative humidity back to 50%, generally done by injecting steam (which in turn counteracts the cooling). In existing installations, energy savings may be accomplished by lowering the relative humidity, by lowering the computer room temperature (particularly when recirculated air is being chilled) or by raising the temperature of the chilled water (where the savings appear in refrigeration-compression costs). In new facilities, the need for emergency electric generators and increased fuel costs can be factored into the original design to achieve an optimum solution.

None of these suggestions should be undertaken without a thorough evaluation by heating and air conditioning specialists through GSA or the building engineer for privately owned facilities. Equipment manufacturers should be consulted if one anticipates lowering the relative humidity significantly, such as to below 35% RH, because of the possibility of static electricity problems.

3.3. Communications Circuits

Increasingly ADP systems are making use of communications circuits for rapid data entry and output. It is important to see that the reliabiliy and integrity of the communications circuits satisfy the requirement of the ADP facility. Figure 15 shows a representative teleprocessing equipment configuration. A specific teleprocessing system may use any one or more of the elements shown in figure 15. As a rule there will be some identifiable hardware unit or units (referred to here as the message processor) which acts as the interface between the computer and the circuits to the individual terminals. Circuits may be hardwired DC circuits or may use modems as shown in the figure. A terminal may be **"stand alone"**, using either a leased line or the dial-up network for access. It may be one of several terminals (usually at several locations) which share a **multi-drop** leased line or one of several low speed terminals (usually at the same location) which **share** a high speed leased line via a **concentrator.** Typically the configuration has been selected to minimize the total direct cost taking into account the cost per minute of dial-up calls, monthly charges for leased lines of WATS lines and lease or capital costs of terminals, modems, etc. However, the cost of delays resulting from communications failures may be significant and provide justification for the direct cost of measures to increase reliability. If the risk analysis has indicated a significant loss potential from delayed processing, the ADP security planner should attempt to estimate the rate and duration of failures and look for remedial measures which can be cost justified. The following are some of the potential failure modes:

One channel of the message processor, one local modem or one telephone circuit to the local central office fails. The result is one channel out of service until the failed element is repaired and, if the channel was in operation at the time of the failure, one incompleted message transmission. If access is via the dial-up network, remote terminals can still access the ADP system, although there may be increased waiting time during busy periods. If access is via leased lines, only the remote terminal(s)* connected to the failed circuit will be affected. A message processor circuit failure cannot be overcome until the unit is repaired

---

* Note that failure of a multi-drop or concentrator circuit will affect more than one terminal.

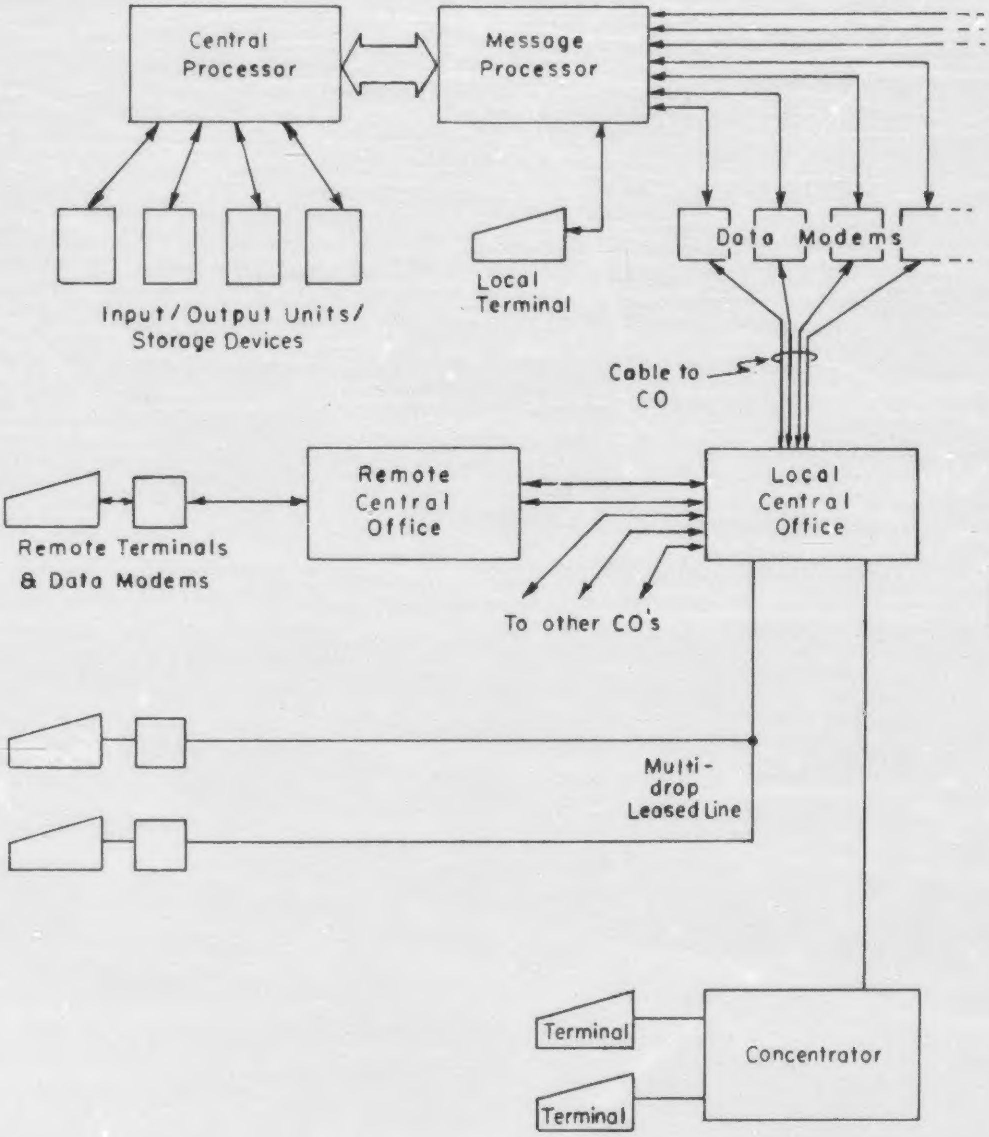

Central Processor
Message Processor
Input/Output Units/ Storage Devices
Local Terminal
Data Modems
Cable to CO
Remote Terminals & Data Modems
Remote Central Office
Local Central Office
To other CO's
Multi-drop Leased Line
Terminal
Terminal
Concentrator

FIGURE 15. *Representative teleprocessing equipment configuration.*

unless there are space circuits one of which can be quickly substituted for the failed circuit.

In general it should be relatively easy to replace a failed modem with a stand-by unit. Repair of a circuit to the local central office will probably be completed within a few hours in most cases but the risk analysis may indicate the need for one or more spare circuits.

The entire message processor, all circuits to the local central office or the central office itself may fail. Any of these result in cutting off all remote terminals and messages being transmitted. A message processor failure is probably the most likely of the three and the repair time may be quite protracted. The ADP security planner should consult with the vendor, review the past history of the unit and attempt to estimate the probable failure rate, and mean time to repair. If the risk analysis supports the cost and it is technically feasible, one may elect to install multiple units which share the common traffic load so that the failure of a single unit will not be catastrophic. By consulting with representatives of the local telephone company or Federal Telecommunications System, the ADP security planner can determine the practicability of installing a separate set of circuits to another central office. While the probability of the simultaneous failure of all circuits to the central office is quite low, it is not zero. In June, 1973 it was reported that thieves had cut the telephone cable leading into a central burglar alarm station. They then broke into and robbed several of the protected premises before the cable could be repaired. This points up the potential exposure to sabotage or vandalism. Cables are also exposed to construction excavation, ice storms, utility pole knock-down, manhole explosions, floods, damage from fires inside the building and earthquakes.

Failure of a circuit from the local central office to a remote terminal or of the terminal itself or its modem. This is the least critical failure since it affects only one terminal and does not impinge on ADP operations. The time to recover from a circuit failure will usually be a few hours for a leased line. Terminal or modem repair time will depend on availability of vendor service support. Based on an estimate of the expected failure rate of the terminal and modem and the mean time to repair, the ADP security planner and the terminal users can project the associated loss potential and so determine if standby equipment can be cost justified. Unless there are many terminals at the remote location or the application is particularly time-sensitive, standby equipment probably will not be justifiable.

This outline analysis of failure modes leads to several points which the ADP security planner should consider:

Dial-up versus leased lines. As a rule one selects leased lines when the amount of traffic reaches the point where leased lines are less expensive than dial-up toll charges or conditioned lines are required because of the data transmission rate. Leased lines lack the inherent reliability and flexibility of the dial-up network. The time urgency of some user applications may justify the cost of additional leased or dial-up lines for back-up. However, it will be necessary to provide the hardware (line switching), software and operating procedures to make full use of back-up lines. Finally, dial-up exposes the system to foreign terminals.

At the same time he is investigating the reliability and mean time to repair of communications circuits, the ADP security planner should examine means to **restore communications** at an alternate site in the event of a catastrophe. The ADP security planner should also consider alternate means to process user input and output, e.g. use of other remote terminals or on-site input-output devices. This information is a vital input to the development of the back-up planning described in Chapter 8.

The ADP security planner should examine the way in which **the teleprocessing software** handles failures. The key points are:

- Recognition of a failure and generation of helpful diagnostic messages at the console.
- Proper handling of interrupted messages particularly as they may affect file updates
- Software flexibility to accommodate a failed channel and the reassignment of users to alternate channels or terminals
- Alternate software to accommodate back-up modes of entry and output.

Finally one should examine the security of communications circuits. Terminal boards and other equipment should be located in locked rooms to which access can be controlled. Cables should be so routed as to protect them against physical damage, preferably by placing them in rigid conduit. Procedures should be established to coordinate telephone system changes and repairs. Care should be taken to show the location of underground cables accurately on ADP facility site drawings and to assure that subsequent excavations are properly planned and supervised to avoid cutting cables by mistake.

Communications circuits are also subject to more subtle tampering. A 1971 newspaper report* describes alleged sabotage of a system by a group of strikers. According to the report, computer polling commands were tape recorded and then transmitted via the dial-up network to remote terminals. The result was to prevent subsequent polling of the terminals by the computer. Twenty-five terminals were affected for nearly a month. This episode suggests the possibilities for what might be called software sabotage. The ADP security planner should review communications software and procedures and if there is significant exposure to tampering, identify modifications which will reduce the exposure, insure rapid discovery and minimize potential damage.

---

* "System Sabotaged by Phone", *Computerworld*, p. 1, December 15, 1971.

Wire tapping; message intercept, alteration and forwarding; access by an unauthorized user via the dial-up network and other aspects of controlled accessibility are not included in this handbook.

3.4. Other Supporting Utilities

Electric power, air conditioning and communications are clearly vital to ADP operations, but other utilities may also be required for normal operations. These are some possibilities which should be examined:

Water supply. Because water is probably required by the air conditioning system and the heating plant, the loss of water pressure may halt operations. A temporary loss of water for drinking and fire fighting purposes probably will not interfere with operations immediately. Water may also be required for processing of microfilm or other photographic media.

Elevators, particularly in high rise buildings, may be important for the movement of people, data and supplies. It is unlikely that all elevators will fail simultaneously except in the event of an electric power failure. However, if it is essential to keep one elevator operating, one must provide an on-site generator which may, of course, also be required for the ADP hardware.

In some large facilities internal **mail conveyors** or pneumatic tubes may be used to deliver source documents or output. It is likely that hand delivery can be substituted, if necessary, but the ADP security planner should verify this and also consider if urgent material in transit at the time of the failure might be trapped in the equipment.

In a few cases, building **heating or air conditioning** may be supported by steam generated outside the building. If this is the case, the ADP security planner should investigate the reliability of the source and the effect of a failure to determine the possible need for alternate sources or for special provisions in the contingency plan.

Building heating or air conditioning may depend on **natural gas** supplied by a public utility. The considerations are much the same as with an external steam source. If an uninterruptible supply is found to be important, the risk analysis may provide cost justification for an on-site back-up supply.

To analyze these and related matters and to examine the cost and feasibility of countermeasures, the ADP security planner should seek qualified professional help from the building manager and other technical specialists available to him.

Because of the interrelationship of heating, air conditioning and electric power, a number of recent buildings have made use of what is referred to as a total energy system (TES). Stated simply, a TES integrates these elements into a single system to provide all three functions. Typically electric power is generated on site and exhaust heat is used for building heating. It has been reported that the overall cost can be less than separate systems and one has the advantage of control over the source of energy. This means that reliability and quality can be tailored to specific user needs. For these reasons, it is worthwhile to consider a TES where planning a new facility, but the ADP security planner should apply the same standards for quality and reliability as he would to conventional systems and be sure that ADP facility requirements will, in fact, be satisfied.

4. Computer System Reliability

4.0. Introduction

Without question, computer reliability is fundamental to ADP operations. However, computer reliability does not always receive adequate attention, often because responsibility for it is not clearly assigned. This chapter introduces three basic areas—reliability of existing computer systems, maintenance management, and procurement of new systems—and suggests ways to deal with them.

4.1 Computer System Reliability

The typical computer is composed of many interconnected units which perform the functions necessary to complete assigned data processing tasks. In the simplest situation, the computer performs a single task and so would probably be configured to use the minimum number of hardware elements required by the task. Thus, the failure of any element would halt operations. In the more typical multi-task environment not all tasks will use all the resources of the computer, and so a failure will not necessarily prevent completion of all tasks. Most computers use an operating system to control the job stream and to allocate memory and peripheral devices to individual jobs. Depending on its features, the operating system will detect failures as indicated by hardware alarms, attempt to localize and define the failure, notify the console operator and adjust its control of the job stream to maximize the number of tasks which can continue to be executed.

Of course, failure of the central processor control logic will usually halt operations. (Note, however, that a failure might go undetected and could disable hardware which controls access.) Likewise the failure of one-of-a-kind peripheral units will interrupt all tasks which use them. Thus failures may permit all tasks to be performed but at a lower throughput rate, may prevent the performance of some tasks or may completely halt operations.

In order to understand the impact of hardware failures on the reliability of ADP operations, the ADP security planner should conduct a system failure mode study by examining the impact of each significant hardware failure. He can do this by noting the computer system resources required by each of the applications identified by the risk analysis as time critical. If the system is at all complicated, he will probably want to consult with staff members responsible for the hardware and operating systems and the vendor's technical support personnel.

The typical ADP procurement will include standards of performance demonstration required for acceptance of a system. Review of the acceptance test documentation will often be helpful to the ADP security planner in estimating system reliability of an existing installation and identifying units most likely to fail.

The objective is to use the failure mode analysis, the loss potential of urgent tasks, and estimates of failure rates and repair times, for projecting future losses to the ADP facility from hardware failures. The projection will permit the ADP security planner to identify those hardware units where failures will be most critical to operations as the basis for the cost justification of remedial measures, as a guide for development of a contingency plan and as an aid in future procurement decisions.

If the analysis shows a significant loss potential from hardware failures, the ADP security planner can consider the following alternatives:

- **Incorporate** one or more **additional units** of a given type beyond the minimum required to perform the stated task load to permit continued operation in the event of the failure of a unit when the analysis shows it to be critical.

- Alternatively, **eliminate a critical peripheral** unit and substitute an alternate technique or procedure. In other words it may be possible that the savings in operating cost resulting from use of a specialized input device might be outweighed by the exposure to losses caused by its failures.

- Take steps to **reduce failures** and speed-up repairs as described in section 4.2.

- **Install two or more computers** which as a group can handle the normal work load. If one computer fails, only the least critical tasks will be interrupted.

- **Install** two (or, indeed, several) **identically configured computers** so that either system can perform all assigned tasks. While this approach (dual or multiple computers) will be difficult to cost justify in most cases, it may be the only acceptable solution for extremely critical or high risk missions.

4.2. Management of Hardware Maintenance

Apart from optimizing the system configuration in terms of achieving established reliability goals, it is important to establish adequate policy and procedures for management of hardware maintenance. Effective maintenance management should include these activities:

- Determine the optimum **schedule and scope of preventive maintenance;** arrange for ongoing supervision to reduce failures to an acceptable level, if possible. As a rule, provisions for preventive maintenance will follow the applicable Federal Supply Schedule but can be modified by mutual agreement between the vendor and the government.

- Report and perform **statistical analysis on hardware failures** so as to detect significant failure trends and take remedial measures on a timely basis. This implies that ADP Operations Branch must report all system failures in enough detail to permit the technical staff to determine the cause of the failure. One ADP facility uses the following procedure: Whenever the system goes down regardless of the apparent reason, a System Incident Report (SIR) is prepared by Operations. The SIR form calls for full information including the time of day, system status, tasks and jobs in the system, diagnostic messages, availability of core dumps and the like. The form also provides spaces for information about routing of the SIR and the final disposition of the incident. At the same time, the incident is added to a log of unresolved incidents by ADP Technical Services Branch. When the incident appears to be caused by hardware, a vendor representative is notified immediately. When the cause is software or unknown, the SIR is passed to the Current Systems Branch for disposition. When the cause of the incident has been discovered, the appropriate agencies take corrective action as needed. The SIR is completed, copies with supporting documents are disseminated to appropriate functions, and the log entry is closed out. This or a similar procedure will insure that problems are discovered and dealt with effectively and that the needed information about system operation is retained.

At regular intervals, the ADP staff member assigned responsibility for system reliability should analyze these reports to identify unfavorable trends. Careful maintenance of meaningful, detailed reports can be of great value. Without them an unfavorable hardware trend may go unobserved for an unnecessarily long period of time and identification of the cause may be further delayed while specific information is being acquired. Full use should be made of error reporting features available in the operating system.

- **Remedial maintenance** should also receive continuing attention. The analysis of loss potential associated with hardware failures may show that efforts to reduce the mean time to repair may be particularly cost effective. Provisions for remedial maintenance are specified in the applicable Federal Supply Schedule but, where the need can be supported by an analysis, the ADP facility may elect to arrange for on-site maintenance personnel or stock piling of critical spare parts.

4.3 Reliability Considerations for New Systems

It is not unusual to find that inherent system reliability receives little detailed consideration in the design of a new system. Paragraph 101-32. 402-7 of the Federal Property Management Regulations [15] defines data system specifications in part as including ". . . a description of the data output and its intended uses, the data input, the data files and record content, the volumes of data, the processing frequencies, timing and such other facts as may be necessary to provide for a full description of the system." What is suggested here is that "such other facts" should properly include a consideration of reliability.

The typical Federal Supply Schedule (FSS) will call for a System Effectiveness Ratio (SER) (operating time divided by operating time plus failure down time) of 90%. It is likely that the system designer accepts this figure for throughput estimates with the realization that work load and run time estimates are of comparable accuracy. Experience suggests that an SER of 90% will be acceptable for the typical batch mode operation but on-line service requires an SER of at least 95%. If the ADP system is involved in life support in any way, a much higher figure is probably required. The ADP security planner should look closely at the characteristics of the planned and likely future work load to test the validity of the system reliabiliy assumptions. Notice that the SER is roughly equivalent to mean time between failures (MTBF) divided by MTBF plus mean time to repair (MTTR). Thus if 160 hours are scheduled for a week (20 eight-hour shifts) one could have eighteen hours of down-time and still achieve a 90% effectiveness ratio. If the nature of the projected work load would make this much down-time unacceptable, additional consideration of reliability is in order. The measures already described for existing systems (dual systems, redundancy within a system and accelerated repair) apply to new systems as well, but it may be easier to apply the first two during system design than after installation.

In cases where the ADP hardware has had significant use elsewhere, it may be possible to get more realistic figures for MTBF and MTTR from the vendor. In such cases, the reliability analysis will be benefited even if it is not appropriate to include reliability figures as contractual requirements. This will be particularly true in the cases where the reliability of a system appears to be marginal based on a 90% SER but corrective efforts cannot be cost justified easily. If credible vendor-supplied estimates indicate that a higher ratio will, in fact, be achieved, one might conclude that system reliability will be acceptable.

Finally one should note that SER does not indicate the duration of hardware failure interruptions. Continuing the example above, one might have one 18-hour interruption per week, six 3-hour interruptions or any other combination limited only by the response time of service personnel. For this reason, the ADP security planner should attempt to determine the likely distribution of interruption durations and examine the implications on performance of urgent tasks since six 3-hour interruptions might not cause any significant loss, but a single 18-hour interruption could be quite serious.

5. Physical Protection of ADP Facilities

5.0. Introduction

This chapter addresses the requirements for physical protection of the ADP facility which can be thought of as the process of permitting access to the facility by authorized persons while denying access to others. It is helpful to think about the problem in three dimensions: **the roles of people**, e.g., computer room operator, ADP programmer, vendor representative; **the criticality of specific areas**, e.g., the surrounding grounds, public areas inside the building, mechanical equipment rooms, the tape library; and **the time of day**, e.g., normal business hours, computer room second and third shifts, periods when the ADP facility is unoccupied. The objective of the physical protection plan is to establish go/no-go criteria for all combinations of these three dimensions and then provide measures to implement them. In other words for each class of individual, the times for which access is permitted is stated for each specified area. To develop these go/no-go criteria, the ADP security planner should conduct a systematic and comprehensive analysis of the threats to which the ADP facility is exposed, the physical characteristics of the building which houses the ADP facility and the organization and mission of the ADP facility. Since the physical protection and controls over access by people will cost money to implement and operate and may represent some impediment to work flow, it is important to try to achieve the optimum level of protection . . . neither inadequate to achieve stated security goals nor needlessly expensive or cumbersome. Likewise it is important to have balanced protection against all determined risks. A senior bank officer recently observed that there was a tendency to build . . . steel doors in paper walls,"* a very graphic description of unevenly applied security measures. For just such reasons the effort to determine protection needs on a realistic basis is well worth the effort.

5.1. Determining Protection Requirements

The first step in the determination is to evaluate the potential threat to the ADP facility from outsiders. Since one is dealing with human motivation there is no easy way to be qualitative. However, one should attempt to make a reasonable determination for each of the classifications which follow. Specifically, consider how both the ADP facility and building tenants will appear to attackers. While determining the likelihood of attack, one should also estimate the likely level of effort the wrongdoer might be willing to exert to achieve his goal.

Common criminals. The concern here is with theft of government property. Would a burglar be likely to think there is valuable property in the building? This might include office machines, firearms, drugs, cash, personal possessions or any other items subject to easy resale or useful for other criminal activities.

Activists. Is the agency active (or thought to be active) in fields which are controversial? Might the building be thought of as a desirable symbolic target at which to direct attention getting demonstrations. An activist group forced entry at a midwestern research laboratory's ADP facility with the intention of destroying magnetic tape data files for research projects of which the group disapproved. No employees were present at the time and the activists did not damage any of the hardware. A number of tapes were said to have been erased and punched cards and the like were thrown on the floor. The group was not discovered during the break-in but revealed themselves at a press conference a few days later. The research laboratory is said to have increased its patrol force coverage and given consideration to intrusion detectors subsequent to the break-in. While damage was estimated to be no more than $100,000 this episode points up the importance to safeguarding an ADP facility against intrusion.

Espionage agents. Does the ADP facility hold or process data which could be of value to an outsider prior to its public release such as economic activity, future allocations of Federal funds or sensitive personal information?

Vandals. Is the ADP facility located in an area where vandalism is prevalent?

The second step in the analysis is to define and tabulate areas within the facility for control purposes. The tabulation should include a statement of the location, function, access requirements (what people at what times), and criticality (contents or activities which may be targets for wrongdoers) for each area. Of course, details will depend on the specifics of the building but these are typical examples of areas which should be considered:

Public entrance and lobby
Loading dock
Spaces occupied by other building tenants
ADP facility reception area
ADP input/output counter area

---

* "IBM, Security Test Sites Vie on Software Strength", *Computerworld*, p. 1, June 13, 1973.

ADP data conversion area
Tape library
Systems analysis and programming areas
Computer rooms
Communications equipment rooms
Air conditioning and other mechanical or electrical equipment spaces

At this point it will be worthwhile to conduct a complete survey of the ADP facility and its environs to determine exposures, to verify security measures already in place and to determine from first hand inspection the state of current practice. GSA provides the following instructions for a physical security survey of a facility (exclusive of internal ADP areas):

5.1.1. Instructions for the Facility Physical Security Survey

A. Obtain a current floor plan which depicts all areas within the facility to include all access points and any adjacent areas belonging to the facility, such as parking lots and storage areas.

B. Begin the survey at the perimeter of the facility and note the following:

1. Property line to include fencing, if any, and type. Condition, number of openings as to type and use, and how secured. Are there any manned posts at the property line.
2. Outside parking facilities. Is this area enclosed and are there any controls? Is the parking lot controlled by manned posts or are devices used?
3. Perimeter of facility. Note all vehicular and pedestrian entrances and what controls are used, if any. Check all doors—number, how secured, any controls or devices, such as alarms or key card devices. Check for all ground floor or basement windows—how secured; screening, bars, etc., and vulnerability. Check for other entrances such as vents, manholes, etc. Are they secured and how? Check for fire escapes—number and location and accessibility to interior of facility from fire escape (windows, doors, roof). How are accessways secured?
4. Internal security. Begin at the top floor or in the basement. Check for fire alarm systems and devices noting the type, location, and number. Where does the alarm annunciate? Check telephone and electrical closets to see if they are locked. Are mechanical and electrical rooms locked or secured? Note any existing alarms as to type and number. Where do the alarms annunciate? Determine number and location of manned posts, hours, and shifts.
5. Monitoring facility. Location who monitors, who responds, type, and number of alarms being monitored.

C. The following questions should also be included in a physical security survey:

1. Is the installation/building protected by alarm system(s)?
2. How many zones of protection are within the protected building?
3. Is the alarm system adequate and does it provide the level of protection required?
4. Are there any vulnerable areas, perimeter, or openings not covered by an alarm system?
5. Is there a particular system that has a high nuisance alarm rate?
6. Is the alarm system inspected and tested occasionally to insure operation?
7. Is the system backed up by properly trained, alert protection officers who know what steps to take in case of an alarm?
8. Is the alarm system regularly inspected for physical and mechanical deterioration?
9. Does the system have tamper-proof switches to protect its integrity?
10. Do system(s) have environmental or protective housing or covers?
11. Is there an alternate or separate source of power available for use on the system in the event of external power failure?
12. Where is the annunciating unit located—local, central station, etc.?
13. Who maintains the equipment and how is it maintained (contract, lease equipment, force account personnel)?
14. Is the present equipment outdated?
15. Are records kept of all alarm signals received to include time, date, location, action taken, and cause of alarm?

16. Are alarms generated occasionally to determine the sensitivity and the capabilities of systems?

When the physical security survey is completed, it should provide a picture of the existing alarm systems and their location and also the number and location of manned posts, the number of personnel at these posts, and their schedule.

With these facts in hand, the ADP security planner can proceed to the evaluation of existing access controls and protection measures, identification of areas where remedial measures are needed and selection of specific measures. The sections which follow describe a variety of useful controls and measures which are included here for general guidance. However, one should seek help from the building manager and the Federal Protective Service (FPS) of the General Services Administration. To the extent permitted by the availability of personnel, the FPS will perform a building security survey on request and can also provide expert advice and guidance on security hardware and the services which can be provided by Federal Protective Officers or contract guards.

The use of various types of devices to augment the existing protective force should be considered. Through the use of such devices, it may be possible to eliminate some of the stationary manned posts at both vehicle and and pedestrian entrances. The manpower thus freed could be directed to other areas or facilities.

5.2. Boundary Protection

The threat analysis may indicate the need to protect the boundary of the property on which the building is located. This may be done by installing fences or other physical barriers, outside lighting, perimeter intrusion detectors or by using a patrol force. Often a combination of one or more of these will be effective. Fencing may be high enough to deter the casual trespasser (three or four feet), too high to climb easily (six to seven feet) or may be intended to deter the determined intruder (eight feet high with three strands of barbed wire). In some cases it may not be necessary to fence the entire area. One may concentrate on key areas such as truck dock areas, parking areas (particularly for nighttime use) or portions of the building which are difficult to keep under surveillance.

Alternatively, one can consider the use of extensive lighting to discourage prowlers. This may be the preferred solution where the threat level is low and fencing is not desired for cost or appearance reasons. Critical areas, entrances, parking areas and locations not covered by existing street lights should receive special attention. In those situations where an entrance is protected by a guard stationed inside, or is used by personnel exiting after dark, it is wise to provide ample exterior lighting. Likewise it is advisable to avoid the use of tinted glass in such locations, as it may be difficult or impossible to see outside after dark.

A third technique for perimeter protection is to use detection devices, usually infrared or microwave beams, which will be interrupted by an intruder. Such devices will cost in the range of $1 to $7 per linear meter and avoid the unsightly appearance of a fence. However, they are not as effective in deterring trespassers, have no value for crowd control, and probably can be circumvented by the skilled intruder. Furthermore, if intrusion detectors are to be useful, one must provide for prompt and effective response by guards when there is an alarm. Depending on the characteristics of the device used and the locale, one must expect false alarms as well. For all these reasons intrusion detectors are of limited value except as a back-up to fencing where a high level of perimeter protection is required or in certain special circumstances where fences are not feasible.

In situations where one is concerned about intruders climbing over or slipping under a fence, one can equip the fence with vibration sensors. One such system uses small sensors mounted on every second or third post and at each gate. Sensors are connected by a continuous wire run to a control panel. Fence motion equivalent to an effort to climb the fence will cause an alarm. The cost is in the range of $1 to $3 per linear meter of fence.

When the ADP facility building is part of a group of Federal buildings and the threat level is judged to be high and fencing is not practical, an outside patrol force may prove to be the most effective protective measure. The composition of the patrol force, its resources (vehicles, radios, dogs, etc.) and standing orders should be carefuly worked out to meet protection needs at least cost. As a rule these decisions will be made by the FPS. The ADP security planner will want to understand the level of protection being provided, and be satisfied that it is adequate to meet the needs of the ADP facility or, if necessary, seek appropriate adjustments.

In some situations, for example, an employee parking lot in a high crime area, it may be helpful to provide a low light-level, closed-circuit television (CCTV) system for nighttime surveillance. Such a system uses one or more CCTV cameras located to cover the desired area and connected to monitors at a central security location. Typically each camera will be on a pan-tilt mount and have a zoom lens, both of which can be controlled from the monitor.

These features will permit the operator to watch a wide area for general activity or to zero in on a particular spot. Depending on installation and specific features, each camera-monitor pair will cost from $4,000 to $10,000 or more. Hardware should be specified by a properly qualified and experienced person. It should be understood that it is unrealistic to expect the operator to watch the monitors alertly for long time periods. Either he should have a schedule for periodic sweeps, or intrusion detectors should be provided to alert him to unusual events. However, a well planned and properly used CCTV system can permit a single guard to monitor a wide area often at a lower cost than a roving patrol.

An exterior CCTV surveillance system can also be of great value for a facility which is subject to demonstrations or other crowd control requirements. Because he can see the entire situation at a glance, the security director can control his security forces in "real time" to assure that the appropriate level of force is applied at all times and to respond promptly to changing conditions. This technique has been used with great success at a major Federal research facility.

It should be noted that prior to the procurement of CCTV equipment for use in GSA operated buildings, proposals must be submitted to the Office of Federal Protective Service Management, Systems Branch, for concurrence.

To summarize briefly:

- **Fences or other barriers** will provide crowd control, deter casual trespassers and help in controlling access to entrances, but it can be costly, will not stop the determined intruder and may be unacceptably unsightly.
- **Intrusion detectors** can alert a guard force to intruders and may be practical where a fence cannot be installed, but they are subject to nuisance alarms, can probably be penetrated by the skilled intruder and require human response to alarms.
- **A patrol force** can provide flexible response (particularly in emergencies), and good deterrence and may be particularly effective for protection of a group of buildings. However, the cost may be excessive.
- **CCTV systems** permit one man to monitor a large area and see exactly what is happening but should be coupled with an alerting function (intrusion detectors or scheduled scanning) and the provision for human response.

5.2.1. Emanations

In evaluating the need for perimeter protection, the ADP security planner should take into account the possibility that electromagnetic or acoustic emanations from ADP hardware may be intercepted. Tests have shown that interception and interpretation of such emanations may be possible under the right conditions by technically qualified persons using generally available hardware. As a rule of thumb, interception of electromagnetic emanations beyond 300 meters is very difficult. However, if the ADP security planner has reason to believe that there may be a potential exposure to interception he should seek technical guidance from qualified vendor representatives. The choice between physical separation of radiating devices from potential intercept points and the use of screening should be based on an analysis of relative cost. Particular attention should be paid to remote terminals which may be located in commercial buildings with non-government tenants.

5.3 Entrance Door Controls

The objective of perimeter protection is to deter trespassing and to funnel employees, visitors and the public to selected entrances. The objective of entrance door controls is to screen entrants, to deny entrance where appropriate and to control the flow of materials into and out of the building.

Screening can be done in two ways: personal recognition of the entrant or acceptance of credentials by a guard[*] or by the possession by the entrant of a suitable device to unlock the door. Screening by a guard is by far the most positive when applied conscientiously but will cost in the range of $2 to $10 per hour per entrance depending on circumstances. Entrant screening can be accomplished by electronic or mechanical devices. Authorized entrants may use a key (conventional or electronic), enter the combination of a push button lock, or be screened by a device which compares an entrant characteristic (hand geometry, fingerprint or voice characteristics) with stored information about authorized entrants. Access control which depends on a key lock or screening device in place of a guard suffers from several shortcomings. Keys or combinations can fall into the wrong hands. An intruder may enter immediately behind an authorized entrant (often referred to as "tail gating"). The skilled intruder may defeat the lock. While these shortcomings can be managed (careful key control, security conscious employees, burglar-alarmed doors, etc.), the ADP security planner should be aware of these problems and not fall into the trap of accepting blanket statements like "This door is always locked", or "This key cannot be duplicated." The features of various door control devices can be summarized briefly as follows:

---

[*] Reference to a guard for screening entrants should be taken to mean any person who has specific screening responsibility and thus may include a receptionist, truck dock supervisor or clerk at a computer in place of a uniformed security guard.

Conventional keys and lock sets. Cost is minimum, less than $1 per key and about $5 per cylinder. Almost any door type can be equipped. However, keys are easily duplicated and locks can be picked. A key holder can enter at any time. There is no control over entrance and exit of materials.

Pick resistant lock sets. Cost is about two or three times higher than conventional locks, keys are much more difficult to duplicate and locks are much harder to pick. Other characteristics are the same as conventional locks.

Electronic key system. These use specially encoded cards to actuate an electric door strike. (With a conventional lock set, the key is used to withdraw the bolt from the strike, thus permitting the door to open. With an electric strike, the bolt remains extended and an electric solenoid retracts the door strike to allow the door to open.) Depending on features and installation, cost will range from about $400 per door to several thousand dollars per door. Cards may cost several dollars each. Simple systems perform as pick-resistant lock sets. At higher cost the system can include the ability to lock out specified cards, to limit access to specified times, to log all entrances and exits, and to control a group of doors such that access to each door in the group can be specified for each card.

Electronic combination locks. Such locks typically have electronic push buttons into which the entrant keys the combination to actuate an electric strike. Costs and features are generally similar to electronic key systems except the entrant need not carry a card. Some allow the entrant to use a special code when under duress which will open the door but at the same time sound a remote alarm. Cost is about $500 per door.

Mechanical push button combination locks. Pressing the correct combination allows one to retract the bolt and open the door. The special features described for electronic locks are not available, but the cost is much lower, typically $40 to $80 per door.

Physical characteristic locks. Cost is in the range of thousands of dollars per door and may require the entrant to carry an electronic key card. These systems come the closest to duplicating human screening in that they measure some physical characteristic of the entrant such as hand geometry, a fingerprint, etc. However the accept-reject decision is made on the basis of an analog input and so some errors will be made, i.e. entry will be denied to an authorized entrant, and vice versa. Furthermore, since such devices are relatively new, it is not yet clear how reliable they are and how easy it may be to circumvent them.

If it is determined that personal screening is necessary at a number of doors and traffic at each is relatively light, it may be cost effective to have a single guard control these entrances with a closed circuit TV (CCTV) system. Each door is equipped wtih a TV camera, a signaling device, an intercom and an electric door strike. To control both entrance and exit it is necessary to have two controlled doors with a vestibule between. This may lead to conflict with emergency exit requirements so caution in planning the installation is required. One commercially-offered system includes a special TV camera which presents a close-up view of the entrant's photo-identification card. By also viewing the entrant on the CCTV monitor and talking to him on the intercom, the guard can screen the entrant almost as effectively as he could in person. Note that he can also monitor movement of materials. The cost for hardware will be in the range of $3,000 to $6,000 per entrance but will be quickly recovered in savings in labor. Since the screening may permit only four or five entrants per minute, one should analyze the traffic patterns carefully, particularly at shift changes, to be sure that there will be no undue delays. Such delay of personnel on an hourly payroll could lead to added expense, a point which should be considered for any unusual screening technique, including CCTV.

It can be seen that at gradually increasing cost one can impose ever more effective screening of personnel and materials. Every effort should be made to establish requirements carefully for each entrance to avoid needless expense and unnecessary entrances should be eliminated if possible.

Each entrance door should be capable of resisting forced or covert entry up to the level of effort which is likely to be applied. This entails careful consideration of door hardware and installation. Where appropriate one may use heavy-duty lock sets, reinforced strike plates and door frames, tamper-resistant hinges and break-resistant glass in vision panels. The ADP security planner should seek advice from qualified persons in this area.

In addition to reinforcing doors one may also connect critical doors to a perimeter alarm system to signal a guard when a door is opened. This can be done for electric strike-equipped doors in such a way that an alarm is not sounded when normal entry is made but forced entry will cause an alarm.

5.4. Perimeter Intrusion Controls

One should check the perimeter of the building for other possible entry points such as windows, transformer vaults, air conditioning louvers, roof hatches and the like. Each point which represents a potential intruder route should be appropriately secured physically or added to the perimeter alarm system. For example, exposed windows can be glazed with break-resistant glass or plastic. Louvers can be protected with heavy gauge screens. The determined intruder may even break through a wall or roof if he feels he will be unobserved for a long enough time period and the target is worth the effort. Where physical protection or adequate surveillance against such forced entry is not practical (as, for example, in a building not controlled by the government) one may install special sensors at windows, loading docks or around the entire perimeter of the building if needed.

The electromechanical type of intrusion detection system is in widest use today. It consists of a continuous electrical circuit so balanced that a change or break in the circuit will set off an alarm. Some examples of systems using a continuous electrical circuit are: foil strips on a window that will break if the window is broken, magnetic or contact switches on the doors, mercury switches on openings that tilt, vibration detectors to detect breaking through walls, and screens and traps which consist of fine wires imbedded in breakable dowels or in the walls, ceilings, and floors. Any tampering with the mechanical parts of the system or breaking or grounding of the electrical circuitry will cause an alarm in the central station. These devices are relatively simple and are normally used for perimeter protection. They may be added to any system (local, proprietary, etc.) without interfering with other detection devices. The various kinds are listed below:

Window foil. Window foil is a metallic tape affixed to windows and glass doors. When the glass is broken, the foil breaks, an open circuit results, and an alarm is sounded. A hairline crack or scratch will activate the system causing an alarm.

Wire lacing and screening. This electromechanical device uses fine wires laced across door panels, floors, walls, and ceilings. A forced entry into the protected area will break a strand of the laced wire which will cause an alarm.

Taut wire. A taut wire device is used to detect intrusion into a protected area. A fine strand of wire is strung under tension across internal openings such as air ducts or utilities tunnels. Any change in the tension of the wire will cause an alarm.

Intrusion switch. A magnet or mechanical intrusion switch is frequently used to protect doors, windows, skylights, and other accessible openings. Switches may be surface mounted or recessed.

- Magnetic intrusion switch. This switch consists of two parts, one being the magnet, the other a switch assembly. When the magnet is properly oriented and mounted adjacent to the switch assembly, the switch is activated. When it is removed the switch is deactivated and an alarm is sounded. Usually the magnet is mounted on the movable portion of the door, window, or item protected.
- Mechanical intrusion switch. This switch is also activated by opening a door, window, skylight, etc. The plunger type switch is usually recessed and costly to install. The lever type switch is less expensive to install but is easily detected. Mechanical switches exposed to the weather may stick or freeze.

In summary, entry into a building is best controlled through either surveillance or high integrity access controls at desired points of entry and by either surveillance or alarm systems around the remainder of the building perimeter. A recent report, "Penetration Tests on J-SIIDS Barriers" [21] shows very graphically how inadequate most structures are for stopping a determined intruder. The report describes actual tests of the time required to make an 8" x 12" opening in a wall, the size judged to be the minimum required by an intruder. Results can be summarized briefly as follows:

Wall Construction	Tools Used	Penetration Time
2" x 4" studs with 1" siding both sides	Hand brace and electric sabre saw	1.55 minutes
8" cinder block wall	Sledgehammer	1.52 minutes*
8" cinder block wall with brick veneer on one side	Sledgehammer	2.12 minutes*
5-½" reinforced concrete	Rotohammer drill and sledgehammer	5.44 minutes*
8" reinforced concrete	Rotohammer drill and sledgehammer	10 minutes approx.*

* Add approximately 1 minute for each reinforcing rod encountered.

5.5. Critical Area Controls

Within the ADP facility, there may not be equal access to all areas even when it is assumed that everyone in the building has been screened through the building perimeter controls. The following areas constitute a minimum set to be analyzed to determine permissible access, both during operational periods and when the facility is closed:

Computer room
Data storage library
Input/output area
Data conversion area
Programmer areas/files
Document library
Communications equipment area
Computer maintenance room
Mechanical equipment room
Telephone closet
Supplies storage

In addition to protecting the confidentiality and integrity of data files, areas should be considered with regard to protecting valuable assets, preventing tampering, vandalism and sabotage, and preventing the perception of opportunities for malice and mischief through unauthorized browsing.

The objective of the analysis is to identify all sensitive or critical areas and determine from a study of work flow and job assignments which persons are to be given access and at what times. The next step is to select control methods. The basic techniques which apply to exterior doors apply here but with two significant differences.

First, it is expected that such areas would be either unoccupied and locked or occupied by authorized personnel. If clear regulations have been published and affected persons properly briefed as described in Chapter 9, then it is reasonable to expect unauthorized persons to be challenged if they enter the space while it is occupied.

Second is the important requirement to avoid impeding work flow unnecessarily. This means that the ADP security planner should examine work flow, people, information and materials carefully in relationship to the physical layout of the ADP facility to avoid obvious problems, such as placing a secured area in the path between two less critical areas. Furthermore, one should try to avoid situations where the designated access route to a controlled area is circuitous and a shorter but unauthorized route (e.g., a fire exit) is available. In such cases there will be a natural tendency to use the short cut. But even when the designated route is convenient, it is not uncommon to find fire exits misused. The common solution for this is to place alarm actuators on fire exit doors. If the facility has a central alarm system, a signal should go to the central system whenever a fire exit door is opened. However, for maximum effectiveness, the alarm should be audible at the doorway. There are self contained alarm boxes which may be mounted on fire doors. The typical alarm is about 10 x 20 x 7 cm in size and has a key actuated arm/disarm switch. When the door is opened, a loud alarm, powered by an internal battery, comes on and can continue to sound until turned off with the key. The cost is approximately $60 per alarm.

The ADP security planner should remember that efforts to control access must not conflict with life safety objectives. The NFPA "Life Safety Code" [30] defines the number, size, and location of fire exits as a function of the building occupancy and construction. It is important to see that there is compliance with such standards and with applicable Federal regulations.

There are several technological means of determining access to or occupancy of critical areas during periods when the areas should be vacant. Two have been discussed: light beams across entrances and CCTV systems. An important caution is that CCTV systems are best used only for a determination of an area's status after there has been an alert from some other, more positive intrusion detector. There are at least four distinct technologies for detecting the presence of an intruder:

1. Photometric Systems. These are passive systems which detect a change in the level of light in an area, due to added sources of light, or reflections or absorptions of existing light. Since these systems are sensitive to ambient light levels, they may be used only in windowless areas (or areas in which the windows have been covered).

2. Motion Detection Systems. The basis for the operation of these systems is the Doppler effect. When the source of a sound or electromagnetic signal, or a reflector of such a signal, moves toward or away from a receiver, the frequency or pitch of the signal received will be higher or lower, respectively. In a room having a source of wave energy and a receiver, if a body moves within that room, the motion can be detected from the change in frequency of received waveforms. The receiver will pick up the source frequency strongly, but will also detect a slightly different frequency at a much lesser strength.

   - Sonic. Sonic detection systems operate in the audible range, 1500 to 2000 hertz and higher. The constant tone is very annoying since it is well within the audio range and at a high decibel (DB) output. This system uses transmitters and receivers (transducers) to saturate the entire enclosure with sound waves. These transmitting and receiving transducers are permanent magnet (PM) speakers and are mounted within the same room, usually on walls opposite each other. The receiver listens to the tone being transmitted and compares the reflected signal. Whenever the pattern of the tone varies due to a disturbance within the protected area, the receiver detects this change in frequency and activates an alarm.

- Ultrasonic. The ultrasonic detection system utilizes high frequency sound waves with a frequency of about 19000-20000 hertz, but are otherwise like the sonic systems. Since the frequencies used are at the upper limit of the audible range, only a few persons (generally children) can hear them.

- Microwave. The microwave system operates in a similar manner to the above systems. The difference is that microwaves are high frequency radio waves. These radio waves are transmitted at a frequency between 400-10,000 megahertz. Microwave signals can be controlled as to the size of the area to be protected through selection of the type of antenna used. One or several antennas can be used in a given location. Single or multiple units can be used to provide the required protection without interfering with sonic or ultrasonic units.

3. The Acoustical-seismic Systems (audio). This system employs microphone-type devices to detect sounds which exceed the ambient noise level of the area under protection. It is obvious that they cannot be employed in areas where noise from man-made sources, such as aircraft, construction, etc., are likely to set off nuisance alarms. Some are even triggered into alarm by the elements, such as rain or thunder. Some acoustic systems rely upon air to transmit the sound to the microphone-type device. Others will not respond to ordinary noises in the air but only to those transmitted through a structure such as a wall.

   - Acoustical (audio). An audio detection system listens for intrusion sounds by using microphones installed in the protected area. Upon detection of intrusion sounds, an alarm occurs. This type of system may be equipped with cancellation and discrimination units which electronically evaluate the significance of the sound disturbance, thus eliminating reaction to nuisance alarms which may be caused by airplanes, thunder, etc.

   - Vibration (seismic). This type of system utilizes the same principle as the audio detection system except that highly sensitive and specialized microphones are attached directly to objects such as safes, filing cabinets, windows, walls, and ceilings. Vibration of these objects initiates alarms. Cancellation and discrimination units are necessary to prevent nuisance alarms.

4. Proximity Systems. There are various types of proximity systems all of which detect the approach or presence of an object or an individual. In principle, a proximity system employs an electrical field which, when upset by a foreign body, causes an alarm. The field may be set up around a cabinet or it may simply surround a wire. Whether the field is electromagnetic or electrostatic, the principle of balance and unbalance applies. There are several methods of establishing the field; methods differ to some extent among manufacturers. A proximity system may also be employed to protect an area by erecting what is commonly known as a magnetic fence; that is an integral part of the system. Other variations provide surveillance of doors and windows.

   The proximity system is designed to be supplemental and cannot be used effectively as a primary system. This is because of the system's susceptibility to nuisance alarms caused by electric supply fluctuations and by the presence of mops, pails, etc., placed near the system. Animals and birds can trigger a system into alarm if it is too sensitive. Therefore, proximity systems should be backed up by other security systems.

The following table compares six of the more commonly available interior surveillance systems:

Sensor Type	Approx Cost	Limitations	Resistance to Defeat
Photometric	$500	Extraneous light must be excluded from area; limited to interior rooms.	High
Motion Ultra-Sonic	$250	Air motion may cause false alarms.	Moderate to High
Motion microwave	$500	Energy can penetrate walls, etc. causing nuisance alarms.	High
Acoustical-seismic. sound	$250	Extraneous noises will generate nuisance alarms.	High
Acoustical-seismic, vibration	$100	Localizing the source of nuisance alarms could be difficult.	High
Proximity, capacitive	$350	Susceptible to nuisance alarms; require backup.	High

In planning the security for critical areas one may make use of the intrusion detectors already described, the controls which can be imposed by guards or personnel assigned to the areas or the physical barriers created by internal partitions. In the latter case, the ADP security planner should check construction details carefully. In modern office buildings using hung ceilings, interior partitions may not extend above the ceiling. This means that an intruder may be able to enter a room by lifting a ceiling panel and climbing over the partition; this is a particularly troublesome form of intrusion since it can be done quickly and quietly without tools and will leave no sign of forced entry. Likewise, interior partition door frames are often of lightweight construction and easily forced open. The key point is not to place undue reliance on interior partitions.

5.6. Guard Force Operations

Physical protection measures, physical barriers and intrusion detectors depend ultimately on human intervention. Where there is a need for full time guards, they will either be Federal Protective Officers provided by the Federal Protective Service of GSA or guards furnished by a private company under contract. In assessing the role guards can play in supporting the ADP security program, it is helpful to review the kinds of tasks which can be assigned to them.

First a guard may be assigned to a fixed post: a lobby, entrance door, truck dock, entrance gate or security control desk. His post orders may include:

- Checking entrant credentials and use of the sign-in log.
- Issuing and recovering visitor badges.
- Monitoring intrusion and fire alarm systems and dispatch personnel to respond to alarms.
- Controlling movement of materials into and out of the building and enforcing property pass regulations.
- Enforcing rules and regulations established for the building.
- Accepting registered mail.

To make optimum use of a guard it is important to see that his post orders are complete and clear and that he is properly trained. For example, if the guard is to control the movement of tapes, disks and other ADP media, he must be able to recognize them and understand what they are. If a guard must devote his time and attention to receiving visitors, preparing badges and telephoning for escorts, he cannot be expected to check employee credentials vigorously at the same time. The ADP security planner who intends to make use of a specific guard post to support the ADP security program, should review the guard's post orders and work load with the building security director to be sure his expectations can be met.

Second, a guard may be a roving patrol guard with a specific route or a general area which he may cover on foot or in a vehicle. His duties may include these functions:

- Verify that doors, windows and other openings are properly locked during designated periods.
- Observe and correct or report safety hazards such as immediate fire hazards, equipment or machinery left on, stumble hazards, fire doors propped open and the like.
- Verify the condition of fire extinguishers, hose lines and automatic sprinkler systems.
- Check that files, safes and restricted areas are properly secured.
- Be alert to suspicious persons or activity, unusual odors, leaks or other abnormal conditions.

If he is to be effective, the roving guard must be under some kind of control. This means either that he reports to a control point at regular intervals either in person or by telephone, or that he is provided with a portable two-way radio. In the latter case he can be dispatched to the scene immediately should an emergency arise. As with the fixed post guard, it is important for the ADP security planner to see that the roving guard has the necessary orders and training to protect the ADP facility properly. For example, if the roving guard smells smoke in an unattended computer room, what should he do beyond giving the alarm? Can he turn off electric power and, if so, does he know where the disconnect switch is located? Similar questions about air conditioning, plumbing leaks and other ADP related emergencies during unattended hours should be analyzed carefully and appropriate orders formulated and guards trained to carry them out.

There is a final point which should be considered when developing the security indoctrination program described in Chapter 9. There is often a tendency for professional staff members to think of the Federal Protective Officer or private contract guard as unimportant and unworthy of consideration. Apart from human feelings, this attitude can nullify the contribution which the guard is depended upon to make to ADP security. ADP management and senior staff members should, by willing compliance with regulations and their general behavior, display their support for the guard in carrying out his assigned duties.

5.7. Integrating Physical Security Measures

The preceding sections of this chapter have discussed the various techniques for providing physical protection. It is not uncommon to find that as each new security or emergency response requirement is discovered (often as the result of a specific event) at an ADP facility, some countermeasures are taken to deal with it. As a result the overall physical protection program evolves piecemeal and so is usually uneven, expensive and cumbersome. On the other hand, a careful examination of the totality of security and emergency requirements, people and procedures will often show how they can be integrated for maximum effectiveness at least cost.

For example, these guidelines have discussed the following kinds of security hardware systems:

ADP area smoke detection systems
Sprinkler system flow alarms
Building-wide fire alarm pull-boxes
Perimeter intrusion detectors
Door status detectors
Critical area intrusion detectors
Area surveillance CCTV
Entrance control CCTV
Electronic door locks

As required by particular circumstances, the physical protection plan may use several of these systems. While one may specify and procure each needed system separately, planning for all requirements as an integrated whole can have two major benefits. First is the requirement for human response to each alarm condition. Consolidating alarm control panels and CCTV monitors in the least number of locations will minimize the number of people required to do this. Second, one may find that more sophisticated alarm controls can be used. One approach uses multiplexor techniques to connect many alarm points to a single control unit via a single circut with substantial savings in wiring cost and improved maintainability. Typically more than one sensor type can be connected to the individual alarm points. More advanced systems use a process-control mini-computer to control electronic access doors, monitor alarm sensors and building mechanical equipment.

In addition to integrating hardware, the ADP security planner, working with the building manager and building security director, should consider the human resources available to support the physical protection plan. In addition to full-time guards, the following people may, as permitted by regular duties, be able to participate:

Receptionists and information desk personnel
Building engineering staff
Building and grounds maintenance staff
Shipping and receiving clerks
Messengers
Area supervisors
Mail room personnel

By considering where such people are located and the needs of the physical protection plan, it may prove possible to get the needed response to alarm situations with a minimum number of guards. However, it can be seen that to do so, thought must be given to the location of security systems, particularly alarm indicators.

We have purposely omitted from this chapter detailed information on security hardware and alarm systems for two reasons. The technology is developing rapidly and new devices appear on the market almost daily. In addition, the Federal Protective Service of GSA can be called upon for detailed advice and expert guidance in meeting specific requirements.

When physical protection plans have been completed, the ADP security planner should check two final points. First, great care should be taken to see that plans and specifications for the ADP facility and its security hardware, alarms, locking systems and related items are protected against disclosure except on a need-to-know basis. Second, the emergency response plans and physical protection measures should be carefully integrated to assure maintenance of security during an emergency. For example, one must guard against the use of a nuisance fire alarm and the resulting evacuation to circumvent controls over access to key areas.

6. Internal Controls

6.0. Introduction

The four preceding chapters have presented physical means for supporting ADP security objectives. This chapter discusses the use of internal controls to reinforce physical safeguards in four areas: personnel, organization structure, the data base and programming. Generally speaking it will not be necessary to cost justify internal controls solely on the basis of expected loss reduction since controls will usually be installed to serve other objectives as well, e.g., cost accounting, error detection and correction, management reports. It is likely that the ADP security planner will find that needed controls already exist and that his task will be to determine what modifications and extensions are needed. The basic risk analysis will have identified sensitive areas and applications. Physical security measures will require human intervention, support and cooperation. The ADP security planner should bear these factors in mind as he reviews the sections which follow to be sure that internal controls are structured to reflect security objectives.

6.1. Personnel Controls

People are undoubtedly the most important part of the ADP facility, and no ADP facility can function without a trained staff dedicated to achieving the mission of the agency. Personnel controls should reflect the need for careful selection of mature, trustworthy people for sensitive positions, the importance of providing adequate training to assume competent performance of ADP duties, and the value of good supervision in achieving a high level of motivation.

6.1.1. Personnel Selection

The selection of personnel routinely includes an effort to determine that the candidate is qualified by training, talent and experience to perform the duties to be assigned. In addition to this determination of job skills, the selection process for sensitive ADP positions should also verify the trustworthiness of the candidate for sensitive positions by appropriate pre-hire screening. Several levels of screening are available and, of course, both effectiveness and cost increase as the depth of the investigation increases. Therefore the level of screening used should reflect the relative sensitivity of each position. Each ADP facility must define for itself its sensitive positions; generally these will include computer operations, data control, management, auditing, and programming (including acceptance testing and maintenance) of critical applications and systems. The risk analysis for fraud will usually identify critical interface points. Wherever a critical interface involves a single indivdual, the postion is probably sensitive. This is especially true for hidden interfaces in which checks and balances are missing, e.g., a single programmer has the responsibility for creating, testing, debugging, and installing a critical program. The most sensitive position is often that of the system programmer; a qualified practitioner of operating system maintenance can do more damage with less chance of being caught than almost any other person involved with data processing.

Each Federal Department or independent agency has established regulations and procedures for designating one or more levels of position sensitivity and the screening applied to each sensitivity level. The ADP security planner should establish the appropriate level to apply to each ADP facility position. Personnel procedures should be established to insure that Item E, Position Sensitivity of Part I of U.S. Civil Service Commission Form 2—Request for Personnel Action, properly reflects the sensitivity levels selected.

6.1.2. Training

A surprising number of operations problems and security breaches result from promoting an individual into a position beyond his competence. Rather than admit defeat, such people have been known to destroy source documents or falsify reports in an attempt to conceal shortcomings.

The ADP facility can use its personnel training program to minimize such security and integrity problems. The training for each specific job should be thorough, efficient, and competent. But strong motivations is just as essential as technical competence. Each employee should be given an adequate orientation to the agency, its mission, the ADP facility and his own career development opportunities. Personalized security training is essential. It should include not only the objectives of the security program and its operation but the duties and obligations of each staff member as well. Details are given in Chapter 9.

6.1.3. Supervision

Each ADP supervisor can make a strong contribution to the security program in several ways. First, he can see that he and his staff comply with both the letter and the spirit of security regulations and control procedures. He can also actively seek out effective ways to to improve security.

Next, the good supervisor will work at maintaining close, effective communications with his staff. He should try to be sensitive to feelings and attitudes so that he can act affirmatively in cases of potential disgruntlement. It is much better to seek resolution of conflict situations than to ignore them, as unresolved conflict can only lead to frustration and impulsive action.

Finally, the good supervisor will take pains to see that each member of his staff is competent in his assigned duties. While incompetence cannot be tolerated in any work situation, the consequences can be particularly pervasive in an ADP facility. A program will faithfully repeat an erroneous instruction indefinitely. A moment of careless operation can damage hardware or destroy a file. Staging the wrong tapes can delay jobs. While errors and lapses can never be completely eliminated, the conscientious supervisor will do his best to match the individual to the job and to give him needed support and training.

6.2. Organizing for Internal Control

One of the basic principles of internal control is to divide the execution of critical functions between two or more persons, a technique often referred to as separation of duties. The theory is that errors are less likely to go undetected when several people review the same transactions and fraud is deterred if there is a need for collusion. One individual should never be totally responsible for a given activity especially if it relates to the processing or development of sensitive applications. This principle of two individuals acting in concert, yet independently, to effect action can be applied to data processing operations. The best approach to determine the exact points where separation of duties should occur is to identify the loss targets by referring to the basic risk analysis for the ADP facility and then to identify the routes to those targets which an intruder could use. Finally, the points along the route can be identified where separation of duties would provide a desirable level of protection. As a rule, separation of duties will be required to control sensitive applications, to prevent compromise of access controls and to avoid abuses in the area of reject and exception processing.

Figure 16 is a generalized diagram of a typical ADP operation with potential control points indicated. The ADP security planner should review each sensitive ADP task to determine where controls would be effective in forestalling errors or fraud and determine how existing controls should be expanded to meet security needs. Consider payroll processing, for example: the controls should insure that input is accurate and valid and that output, paychecks, payroll journals, etc. do not fall into the wrong hands. If the payroll is large, exception processing is probably important. Therefore, the clerk who prepares input should not control check signing and distribution or corrections to the payroll file. Similarly, the programmer who maintains the payroll program should not control its acceptance testing. These examples are much simplified, of course. The real exposures are often hidden from direct view. The key point is to examine each potential target and identify the points in the work flow where separation of duties can help to stem losses.

Many applications are designed for the rejection of invalid input and its correction and re-entering. While this is a valuable quality control technique, the introduction of manual processing of rejects offers significant opportunity for fraud as well as errors. A useful control for rejects processing is the use of a system-generated log or a bookkeeping journal record to keep track of all incompleted transactions. These records will provide an independent audit trail for control purposes, and separation of duties should apply to the clearing of the log. Someone other than the person responsible for correcting faulty input should initiate the transaction to clear log entries.

Program and procedure change controls should receive special attention from the ADP security planner. The process of getting a program from test to production status exposes the system to compromise from unauthorized changes and to loss of data integrity caused by too hurried development or inadequate testing. The ideal approach to installing a change in a production program is a formalized system in which several different organizational functions are involved. User, programmer, auditor, and operations personnel should all be involved in the approval process. Quality control of programming is as important a concept as quality control in manufacturing. An organizationally discrete checking and follow-up function can be of value in maintaining program quality standards. In addition, the larger ADP facility should consider establishing a separate testing function for all programs that have reached final production status.

Since controls are managed by people, the basic organizational structure must be responsive to the desired internal controls. Figure 17 shows a prototype organization chart. Note that the key control functions: testing and quality control, project management, input/output control, tape disk library and standards, security and data base administration have been separated from the production functions. This makes it easier to assure that checks and controls will function effectively. Of course, the details for a specific ADP facility will depend on its size and mission. While the major problem for a large ADP facility is often effective control of resources, the major problem for the small ADP facility may be the practical problems of having enough different people available to implement desired separation of duties. If this is the case, and it is necessary for one or more individuals to have an unusually wide span of control, it may be necessary to depend on auditing. This presumes that good audit trails are provided.

To summarize, the following points have been made:

- Take great **care in selecting personnel** for sensitive ADP positions. Be sure that each person receives ample training and close, effective supervision. These measures will provide the basis for a strong ADP staff.
- **Analyze the tasks** performed and assets controlled by the ADP facility to identify the targets and mechanisms for damaging errors or fraud.

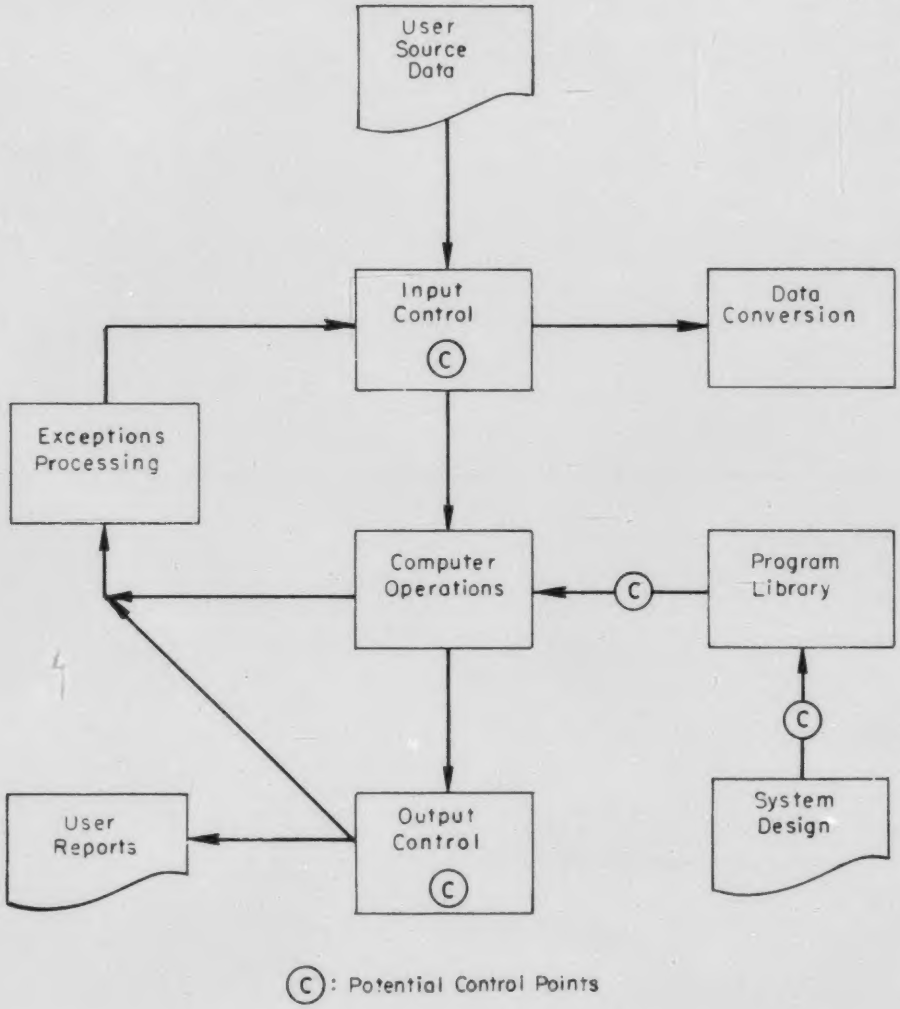

User Source Data
Input Control
C
Data Conversion
Exceptions Processing
Computer Operations
C
Program Library
C
Output Control
C
User Reports
System Design
C : Potential Control Points

FIGURE 16. *Work flow and control points.*

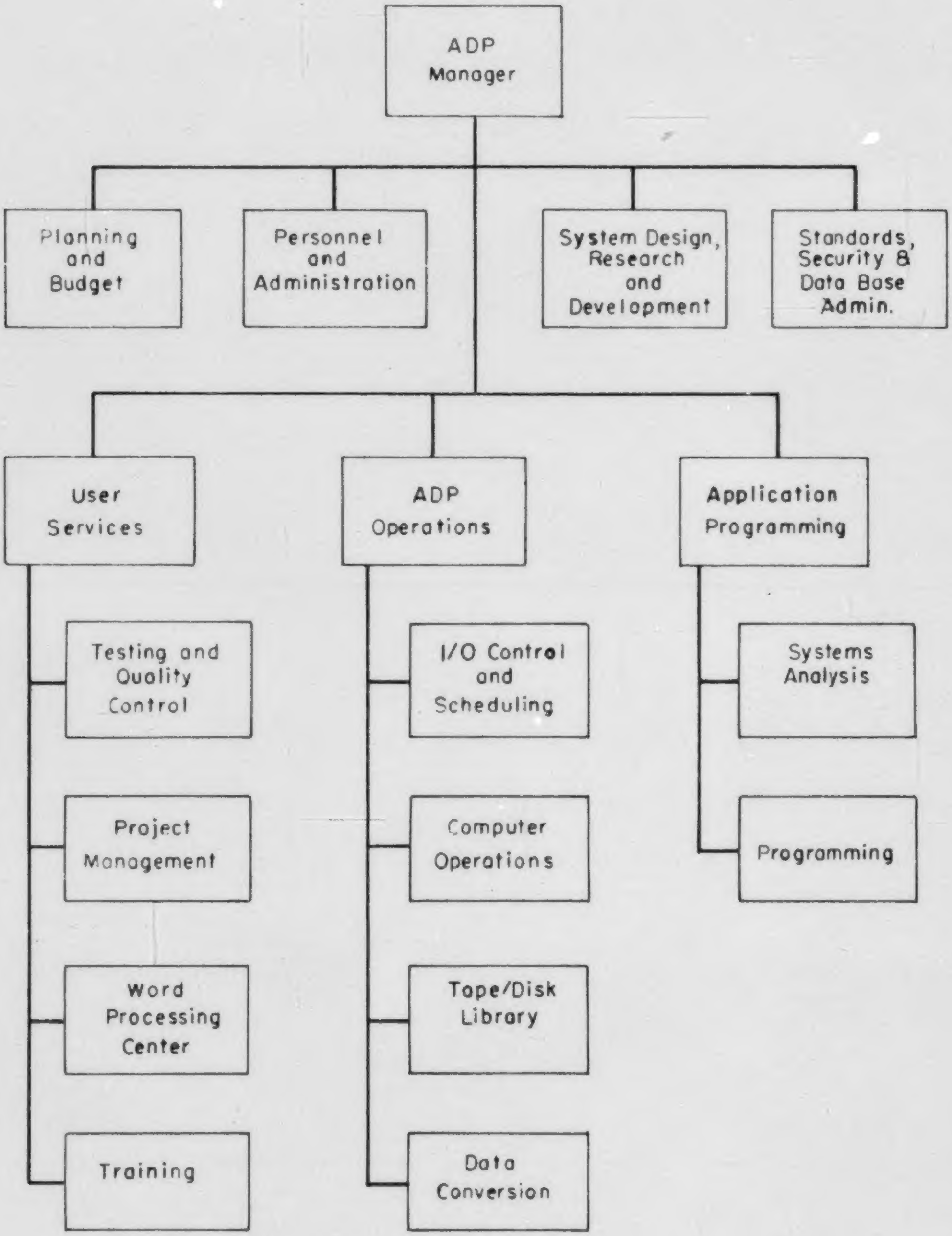

ADP Manager
Planning and Budget
Personnel and Administration
System Design, Research and Development
Standards, Security & Data Base Admin.
User Services
ADP Operations
Application Programming
Testing and Quality Control
Project Management
Word Processing Center
Training
I/O Control and Scheduling
Computer Operations
Tape/Disk Library
Data Conversion
Systems Analysis
Programming

FIGURE 17. *Prototype organization chart.*

- To the extent permitted by the size of the ADP staff **use separation of duties** at key control points to minimize errors and deter fraud.
- **Augment** separation of duties **with internal controls** as appropriate to meet the security objectives.

6.3. Data Controls

Apart from conventional internal controls, the ADP security planner should particularly verify control and protection of data files. Care must be taken to see that information which has been designated as sensitive under Federal regulations is properly safeguarded when it is entered into ADP data files. This may require special handling, segregation or other techniques similar to those used for national security information.

The ADP security planner should also evaluate physical handling of data files at all points. He should examine the flow of data through the ADP facility to identify points at the input/output interfaces, during handling, and during custodial storage, where controls may be needed to safeguard against possible loss or destruction —and equally important to assure that a loss will be detected. The ADP facility should follow defined procedures in case data is lost. Manual control techniques might include tape/disk movement control forms, inventory logs, authorization for use and special handling for critical items.

The use of a computer system for control of data files deserves special consideration if there are a large number of files. Many vendor supplied tape or disk library management systems provide logging and control of tapes by volume, serial number and name; prevent unauthorized destruction of a data file; and provide automatic backup facilities. Such systems handle both on-line and off-line files.

Similar systems are available to manage a program library. The typical system allows continual modification of a program which is being developed while retaining all previous versions. It protects against unauthorized modification, and helps with the management of program modifications. Such packages, whether purchased or developed in-house can be very useful for management and control of data and program files.

In pre-computer days it was axiomatic to lock up sensitive or important information, ledger books and vital records in a desk drawer, file or safe when not in use. The same principle should also apply to valuable computerized data. The tape library should be locked when unoccupied and unauthorized persons should be excluded. Data safes and vaults, and data control rooms should be protected in accordance with the sensitivity and value of the material (data) stored within. The exposure to magnetic fields should be evaluated realistically [12] and reasonable protective measures taken. Computer printouts should be destroyed in accordance with sound procedures to prevent disclosure. It does little good to develop extensive security controls against theft of data from the computer or programming area and then allow the same information to be available from waste baskets, loading docks or trash heaps. The ADP security planner should be sure that data control requirements are properly reflected in the physical protection program described in Chapter 5.

6.4. Data Retention and Back-Up

The preceding section has discussed protection of current data files. The next step is to integrate the vital records management program with the data base management program to support common retention objecitves. Generally speaking both short term and long term back-up is required.

6.4.1. Short Term Back-Up

Short term back-up protects against localized or temporary loss such as cancellation of a job because of an interruption or error. The interruption may last only a millisecond, and the program (especially if it is a short one) may be re-run easily. However, if the job is interrupted in the thirteenth hour of a fourteen hour processing job, it would be wasteful to have to begin the job again. Therefore, checkpoints, restarting, recovering, and backup at intermediate points need to be considered for all long jobs. This is not news to anyone operating ADP facilities. Nonetheless, a consistent backup program is rarely found.

In determining short term back-up requirements, cost considerations play a large role. For example, assume one could checkpoint at any time at a cost of **X** dollars. If the total job costs **X** dollars to run, it would not be cost effective to use any checkpoints. If it costs **200X** to run the job, it would probably be sensible to back-up the data at intermediate points. A review of system reliability as described in Chapter 4 may be of help in making the best decisions.

6.4.2. Long Term Back-Up

There are six reasons why one would want to retain a past environment:

1. Discovery of errors that caused data integrity problems in the past, e.g. to trace a series of mistakes going back six months but not discovered until yesterday.

2. Back-up which permits disaster recovery. These situations are covered in detail in Chapter 8.

3. Management performance review or planning. The future goals and activities of the ADP facility can be predicted more easily if information on past activities can be retained. Use of simulation models or other planning tools is enhanced if empirical data is used as input.

4. Statistical reporting requirements. Data from the past may be needed for analysis of trends and for extrapolations.

5. Audit requirements (internal and external). The ability to analyze the past environment is a primary requirement of the auditor. Specific requirements are discussed in Chapter 10.

6. Legal requirements. Other government agencies may need the data or there may be a statutory requirement to retain them.

Any of these reasons would dictate that one should keep at least program source code, documentation and data files which were in use at any given point in time. The ADP security planner should give thought to what is to be retained. Should it be the entire operating system configuration, all documentation, compiler, execution job language programs and data files? Or should it be just the changing elements of the processing? Once he decides what is to be retained, he must also decide how to retain it. A good outline of advanced techniques is available in "Reliability of Real Time Systems" [60-65].

6.5. Programming Controls

In line with the recognized objective of generating technically sound programs, the ADP security program should include controls in the areas of program design, acceptance testing and standards. Each of these topics is discussed in the following sections.

6.5.1. Program Design

There are five major program areas in which design can contribute to security. First is the inclusion of audit trails in the programming process. The basic objective is to make it possible at any point in time to determine the status of a given piece of data. In most cases the systems analysts and system designers will want to involve the auditor in the design phase as he will be able to postulate the optimum placement of audit trails and controls.

The second is the development of a test plan that will consider all possible elements of input, and the interfaces and operational aspects of each new program as part of the program design effort rather than as an afterthought. It is not enough to test a program for ranges of likely input; it should also be tested for improbable, illegal and impossible input. In addition, stand-alone tests usually are not sufficient to establish the adequacy of a given program or module. Not all programs need to meet the same test criteria; the stringency of the testing should be a function of importance, complexity and sensitivity. Development of written testing guidelines tailored to the needs of the ADP facility is an important step in achieving good control.

The third control area is program change. Programs should be designed to simplify installation of future changes. Every change, even those involving only one statement, should be authorized, approved, and documented with no exceptions. Otherwise, control is lost and the programming process becomes anarchistic. Program library maintenance packages, as mentioned previously, can help in the control and maintenance of program changes. Naming conventions are essential to program change control. The current trend is toward integrated data definitions for all ADP applications, so that every element will be unique.

Controls on the accuracy of data records are the fourth design objective. There are a wide range of possible checks including keypunch verification, computer matching against predetermined legal values for fields, self-checking digits and control fields. Standard design criteria should include the qualitative controls to be included in any new application or any revision of an old application.

Finally, quantitative controls where feasible should also be installed during the design process. These could include control totals, run-to-run counts (hash totals), trailer records, dollar controls, automatic check-points/interruption routines, verfication of the output and input record counts and the like. Violation of qualitative and quantitative controls should cause error notifications maintained as an error suspense file.

The need for quantitative and qualitative controls should be determined by the risk analysis. If the application is of high value, high risk, or consumes a great deal of ADP resources, these controls should receive more attention than low risk, low visibility applications.

6.5.2. Program Installation

One of the most sensitive points in the programming process is the release of an application to the production system, and its operation against a live data base. Installation of a new program should occur only after thorough program and system tests have been completed and approved. The more organizational entities participating in this approval, the better the control. The programmer, a testing or quality

Symbols:
I: Initiates document
A: Approves document
U: Uses document

		User	System Design	Programming	Job Control	Operations	ADP Management
Feasibility Study	Study Request	I	U				A
	System Requirements	I	U				
	Cost and Schedule	A	I				A
System Design	System Flow Chart & Narrative	A	I	U	U		A
	Source Documents & Input	A	I	U	U		
	Record and File Organization		I	U	U		
	Output & Reports Formats Instr.	A	I	U	U	U	
	User, Keypunch & Control Instr.	A	I	U	U	U	
Programming	Program Narrative & Flow Chart			I			A
	Coding			I			
	Program Test Req's & Schedule			I	U		A
System Test	Test Requirements & Schedule	A	I	U	U	A	A
	Test Report	A	A	A	I	A	A
Implementation	Implementation Schedule	A			I	U	A
	Data Conversion Plan				I	U	A
	User Acceptance	A			I		A
Operation	Program Maintenance		I	U	U		A
	Program Modification	I	U	U	U		A

FIGURE 18. *Matrix of Suggested documentation to control and record programs.*

control function, operations, and users should all participate in getting the program from design to final acceptance test and into the live system. However, care should be taken to see that approval does not become a mere ritual. Each program should receive detailed, independent review. Larger ADP facilities may want to consider establishing a separate program test and control group. Smaller ADP facilities would probably be served adequately by defining specific procedures for the installation process to be carried out by an existing group but with as much review and separation of responsibilities as is possible. Again, no program should be accepted without adequate and complete documentation which has been reviewed and approved by an independent body. In case of disaster or non-availability of key programmers, the ADP facility could find itself quite vulnerable to loss if the documentation is inadequate. Figure 18 shows a suggested set of documentation which will provide the needed controls as well as technical information.

6.5.3. Documentation of Controls

The procedural controls over data, operations, system design, programming and acceptance testing already described must themselves be documented if they are to be fully effective. This is often done by preparing documents called procedures manuals, operations and user handbooks, or similar titles. Responsibility for producing the documents may be assigned to a procedures group in a large ADP facility. The small ADP facility may call on individuals to document their particular areas. In either case, the ADP security planner should participate. He should analyze the security objectives of the ADP facility as discussed above to determine the role of the practices or standards in accomplishment of security goals. Based both on these security objectives as well as on ADP management goals, a procedures program should be formulated for the ADP facility. An example of a table of contents for a programming procedures manual is included as Appendix C.

7. Security of Off-Site ADP Facilities

7.0. Introduction

There are four basic reasons for making use of an off-site ADP facility:

1. The ADP needs of an agency are too small to justify an in-house ADP facility. A business whose routine data processing is done most economically at a service bureau serves as an example.

2. The efficiency and economy of the on-site ADP facility is enhanced by doing peak-load processing at an off-site facility.

3. A special service may be available from an off-site ADP facility which cannot be provided economically by the on-site facility. Use of an interactive time-shared computer for special jobs is characteristic of this usage.

4. In the event of catastrophe or major damage to the on-site ADP facility, critical ADP tasks are moved to a preselected off-site facility for back-up operation.

The first three represent routine on-going use which is likely to increase over the years ahead. The fourth use results from the working of a contingency plan for an in-house ADP facility or as back-up for an off-site ADP facility. What is recommended here is that the basic security considerations presented in these Guidelines for on-site ADP facilities be applied equally to off-site ADP. This chapter will address the problems that the ADP security planner must face in evaluating the security of off-site ADP. Fundamentally, the user of off-site ADP is in a position very similar to the depositor in a bank—that is, the protection of one's assets is turned over to another organization. Unfortunately, the user of off-site ADP does not have the protection provided to the bank depositor: the law, independent audit, and the FDIC. In fact, most ADP service bureaus provide a uniform (and often undefined) level of security at best for all of their users regardless of individual user security requirements. As a rule the typical ADP service bureau does not guarantee any specific level of security protection for users and does not accept responsibility for the losses that the users might incur because of data theft, processing delays or other disruptions. For these reasons it is not safe for the user to assume that work processed at an off-site ADP facility is being protected by adequate security measures. The conclusion is this: the fact that an agency does some or all of its data processing at an off-site ADP facility (the operation of which the agency cannot control) does not relieve the using agency of responsibility for protecting its own data against loss or misuse and for avoiding delays in processing which interefere with accomplishing its mission. Indeed, the fact that the using agency cannot control security directly makes the analysis of security even more important. Therefore, it is recommended that an agency which uses off-site ADP facilities, support an ADP security program as described in this chapter.

If a combination of on-site and off-site ADP is used, then the person responsible for on-site ADP security planning probably should be responsible for off-site ADP planning as well. If there is no on-site ADP facility, then the ADP security planner might best be chosen from the office responsible for vital records management, or the major ADP user in the agency. The designated ADP security planner should seek support and participation from all ADP users in the agency and advice and counsel from specialists as suggested in section 1.3.2.

7.1. Analysis of Security Requirements

While the basic techniques for risk analysis described in section 1.3 apply, the following approach may be helpful when off-site ADP facilities are being used:

- **Develop a loss potential** estimate for the using agency as described in section 1.3.

- **Perform a threat analysis** as described in section 1.3.2 but note that instead of a single environment (the on-site ADP facility implicit in the discussion in section 1.3.2), one must, in general, consider four different security situations and environments as follows:

1. Protection of source documents, data files, ADP documentation data entry and output hardware, and related items while they are in the custody of the using agency.

2. Protection of data while in transit in either direction between the using agency and the off-site ADP facility. Note that data may be transmitted either electronically or physically (as source documents, machine readable media or output reports).

3. Security of using agency ADP operations at the off-site ADP facility. The using agency may participate in an existing security program managed by the off-site ADP facility or may prefer to develop and maintain its own contingency plan to protect its off-site ADP operations.

4. Protection of data, preprinted forms and other materials stored at an off-site location in support of the back-up operations plan of the using agency.

- **Develop an annual loss expectancy** estimate as described in section 1.3.3. The basis for the estimate will differ from the single site situation in a number of ways. The using agency does not suffer a loss from the destruction of physical assets (other than its own tapes, disk packs, etc.) at the off-site ADP facility. Similarly destruction of data files and other material at the back-up site results only in the cost to replace them. These considerations are summarized in the table below for each of the five loss-potential types listed in section 1.3.1. A **Yes** entry implies a loss potential similar to a full on-site ADP facility, a **No** entry means that the loss mechanism does not exist and the entry **Minor** refers to a loss limited to the relatively minor cost to replace data, documentation and related items.

The ADP security planner should test the validity of the assumptions in the table for his particular situation so as to be sure that his loss expectancy estimates will include all significant factors.

Potential Loss Type	Loss Location			
	On-Site	In Transit	Off-Site	Back-Up Site [e]
Physical Loss	Yes[a]	Minor	Minor	Minor
Data Loss	Yes	Yes	Yes	No
Data Theft	Yes	Yes	Yes	Yes
Indirect Theft	Yes	No[b]	Yes	No[c]
Processing Delay	Yes	Yes	Yes	No[d]

[a] The potential is probably much lower than for a full on-site ADP facility since hardware is limited to remote terminals.

[b] It is assumed that tampering with data in transit would not go undetected.

[c] It is conceivable that an embezzler might be able to tamper with inadequately protected back-up files and then destroy on-site files to force the use of the back-up files. However, this seems to be a rather farfetched fraud scenario.

[d] If back-up materials were destroyed by the same event as the operational site, i.e., at the same time, a processing delay would occur. Hopefully, the back-up site has been selected to minimize the probability of a joint disaster as might occur if the operational and back-up sites were located on the same earthquake fault line.

[e] Note that the using agency may elect to use its own facility to store materials to back up operation at the off-site ADP facility.

7.2. On-Site Security

Analysis of the security of the on-site portions of ADP operations is conducted as has been described in the preceding chapters of this handbook. Obviously if processing is done off-site, the ADP security planner need not concern himself about protecting an expensive, complex ADP facility, but he will want to consider points like these:

- Physical protection, access controls and data **controls for source data** at the point where they are concentrated enough to become a target for wrongdoers or where responsibility for data integrity shifts from users to ADP operations.

- **Protection of remote terminals** against threats such as misuse or sabotage (deterred by physical access controls), damage caused by fire, flood, etc., or delays in processing caused either by physical damage to the terminal or by interruptions to electric power or communications circuits.

- Physical protection for data files, documentation and other back-up materials which may be **stored on site.**

7.3. In-Transit Security

The security analysis should consider the exposure while data and documents are in transit. Except for interception of electronic data transmission which is excluded from the scope of this handbook, the following points should be considered:

- **Physical loss of input.** Where the cost to reconstruct or the loss from delayed processing is significant, steps should be taken to permit prompt replacement of input which is destroyed or lost in transit. Accidental erasure of magnetic media is unlikely and is easily protected against by using magnetically shielded shipping containers. Heat, x-rays, and radar are all overrated threats which can be managed with common sense precautions based on a technical report by 3M Company [19] and an NBS report [12]. However, there is always some exposure to these threats and to the possibility that a shipment will be misdirected or otherwise go astray.

- **Physical loss of output.** Output which will be in the form of printed or microfilmed material is subject to the same exposures as ordinary mail but it obviously can be protected by the simple expedient of retaining the output data file at the off-site ADP facility until delivery has been confirmed. Alternatively, one might prefer to trigger replacement on a report of non-delivery. In other words, unless non-delivery (the less common event) is reported by a specified time, the off-site ADP facility assumes delivery has occurred and need not retain the output file any longer (although exception reporting in this case carries greater risk than reporting each delivery).

- **Protection against disclosure.** The loss potential analysis may show that either input or output are sensitive and must be protected against wrongful disclosure. Presumably the degree of protection required can be related to the value of disclosure to potential perpetrators and to the level of effort they are likely to use. Protection techniques used for classied materials while in transit can be used as guidelines for developing protection techniques for unclassified but sensitive information.

- **Protection against tampering.** The loss potential analysis may show that either input or output is subject to tampering for fraudulent purposes. Protection of input can make use of the same controls, in general, as are applied to in-house processing. However, one must take pains to see that steps are taken to protect not only input data, but control informaion as well. This is because one might conceal input data tampering by compensating changes to control data. Ideally, control information is kept on-site and output is not released until it has been verified against the on-site control data. However, if time constraints require verification at the off-site ADP facility, then control information can be protected while in transit. One may depend on the deterrent value of ultimate, if delayed, detection of tampering through later on-site confirmation.

The ADP security planner should bear in mind that in many instances frauds have been concealed by substitution of altered output. For example, a recent report described how diversion of funds from dormant bank accounts was concealed by sending altered statements to the dormant account holders. The fraud was discovered when a delay in processing prevented the embezzlers from making the substitution.* This episode points up the situation where the fraud is revealed only by detailed output reports and so may be concealed (for a time at least) by tampering with these output reports. It seems likely that output which is shipped from one site to another for distribution, would be particularly subject to substitutive tampering.

7.4. Off-Site Security

The same technique is used to analyze security at an off-site ADP facility as has been described for an in-house ADP facility but with a variation in emphasis as a result of variations in the loss potential. For example, if we estimate that we will operate 0.5% of the time at the back-up site, delayed processing losses would likely be on the order of 0.5% of their equivalent at the ADP facility normally used. In other words, the less likely we are to be operating at the back-up site, the less significant its reliability is to us so that we can place more emphasis on such factors as availability, process integrity, technical compatibility and convenience in evaluating it.

The emphasis for an off-site ADP facility which is used regularly would be the same as for an on-site facility, with the exception that one's concern is obviously limited to one's own assets. The ADP security planner can begin his security analysis of the off-site ADP facility by reviewing as much of the following documentation as is available from the off-site ADP facility:

- a copy of the latest **risk analysis.**

---

* "DP Figures in Bank Loss of $128,000," *Computerworld*, p. 1, February 3, 1973.

- a copy of the **contingency plan**—when it was last updated and the last time it was tested.

- a copy of the last **security audit**, its date, and who performed it.

- a copy of the **security policy** and procedures.

- a copy of all other ADP **physical security documentation.**

On the basis of the available documentation, an inspection and survey of the off-site ADP facility, and his own estimate of his agency's loss potential, the ADP security planner should be able to draw one of the following conclusions about the off-site facility:

1. The security program at the off-site ADP facility is acceptable and no separate back-up arrangements are required. Presumably, the using agency will participate in and cooperate with the security program at the off-site ADP facility.

2. Protection of using-agency data and other materials is adequate, but reliability and contingency planning are inadequate; i.e. the exposure to processing delays is judged to be unacceptable. If the using agency finds that it can develop and maintain its own back-up plan, then use of the off-site facility could be justified despite the less-than-complete security program. However, the cost of the independent back-up plan should be factored into the price/performance evaluation of the off-site ADP facility.

3. Security at the off-site ADP facility is judged to be inadequate. In this case it may be possible to arrange with the management of the off-site ADP facility for either a general upgrading of security, if that is what is needed, or installation of special measures for the using agency, such as special handling of using-agency data. However, when management is unwilling or unable to upgrade security, the using agency will have to look elsewhere for ADP services.

When the risk analysis has been completed and an off-site ADP facility is selected for use, the using agency must support its ADP security program as described elsewhere in this handbook. Specially, the following should be covered:

1. Security policy and procedures should be documented.

2. Using agency personnel who have ADP security responsibilities should receive appropriate indoctrination, training and supervision.

3. An ADP security audit program should be established. The using agency may find that it can place reliance on audits performed by the off-site ADP facility for part, if not all, of its audit needs.

8. Contingency Planning

8.0. Introduction

Each agency of the Federal government has an assigned mission. Plans are prepared and executed for the accomplishment of that mission. These plans assume normal working conditions, availability of the agency's resources and personnel and a tranquil community atmosphere. Even so, the ADP security planner recognizes that despite careful use of preventive measures there is always some likelihood that events will occur which could prevent normal operations and interfere with accomplishing the agency's mission. For this reason, he should include contingency plans in the ADP security program.

Three different types of contingency plans are required for an ADP facility:

Emergency response. There must be procedures for response to emergencies such as fire, flood, civil commotion, natural disasters, bomb threats, etc., in order to protect lives, limit the damage to property and minimize the impact on ADP operations.

Back-up operation. Back-up operation plans are prepared in order to insure that essential tasks (as identified by the risk analysis) can be completed subsequent to disruption of the ADP and continuing until the facility is sufficiently restored.

Recovery. Recovery plans are made to permit smooth, rapid restoration of the ADP facility following physical destruction or major damage.

8.1. Preparation of Contingency Plans

Because good contingency planning is an important contribution to stable ADP operations and will require substantial effort, it is recommended that a formal task force be established with well defined goals and a budget and schedule as a part of the security program implementation described in section 1.4. Furthermore, it will be necessary to have the participation of qualified people from other areas. Figure 19 suggests how tasks might be set up and assigned. Of course, each ADP facility will want to adapt to its own special circumstances and make full use of the resources available to it.

Tasks	ADP Management and Security Planner	User Representatives	Building Management	Building Security	Agency Legal Counsel	Procurement Division	Public Building Service (GSA)	Agency Auditors	Agency Management	Refer to section
	TASK FORCE MEMBERS									
1. Establish task force	●								●	8.1
2. Estimate recovery time	●		●			●	●			8.1
3. Failure mode analysis										8.1
ADP hardware	●									4.0
Utility failures	●		●							3.0
Fire, flood, etc.	●		●	●						2.0
4. Loss potential	●	●			●			●	●	1.3
5. Emergency response plans	●		●	●	●				●	8.2
6. Selection of back-up modes	●	●		●	●			●	●	8.3
7. Recovery plans	●	●	●			●	●		●	8.4

FIGURE 19. *Organization and tasks for contingency planning.*

The selection of modes of back-up operation (Task 6) depends in part on two basic factors. The time required to recover (Task 2) fixes the maximum duration of back-up operation. The loss potential associated with the individual ADP tasks (Task 4) fixes the maximum duration of an interruption to processing which will not cause a significant loss. If the disruptive event is expected to last longer than this time, back-up operations should be initiated.

The failure mode analysis (Task 3) enables the ADP security planner to identify the events which are likely to precipitate back-up operations. Basically, the approach is to relate the threats identified by the risk analysis to the three major classes of effects: limited loss of capability, interruption to operations and major damage or destruction. Tabulating the effects, as shown, may be helpful:

Effect	Typical Causes
Limited loss of ADP capability.	1. Failure of key peripheral hardware unit(s). 2. Partial loss of air conditioning, etc. 3. Communications circuit(s) failure. 4. Loss of key programs, files, preprinted forms. 5. Non-availability of key personnel.
Interruption to ADP operations, little or no damage to facility.	1. Labor disputes, demonstrations, civil commotion. 2. Failure of electric power, air conditioning. 3. Evacuation caused by bomb threat, gas leak. 4. Failure of major ADP hardware unit. 5. Computer room fire, sabotage of ADP hardware, localized flooding. 6. Intrusion of smoke, dirt or dust.
Major damage or destruction of ADP facility and contents.	1. Major fire. 2. Earthquake, general flood, tornado. 3. Bombing, explosion, aircraft crash.

The significance of each of the three effect classes shown in the tabulation is as follows:

Limited loss of capability implies that only some tasks will be affected. To evaluate the need for back-up, the ADP security planner must relate each cause to the affected ADP tasks. These tasks will differ in time urgency and loss potential. For example, consider the situation in which an optical character reader (OCR) unit is used to enter data from source documents. If the mean time to repair were significantly shorter than the cycle time of the task(s) using the OCR unit, one would probably conclude that no back-up was required, particularly if there was ample catch-up time for all OCR jobs. On the other hand, if the OCR unit operated three full shifts per day, the need for an alternate data entry method would be obvious.

Another example would be a partial air conditioning failure. Assume that the computer room has three identical air conditioning units, it has been determined that the mean time to repair is eight hours and the room temperature will exceed allowable limits in 30 minutes. If enough ADP hardware and room lighting is turned off, temperature can be stabilized at an acceptable level. The ADP security planner should check the list of tasks for which an eight hour delay will cause losses to see if there is a subset of the normal computer configuration having a heat load which will allow these tasks to be completed. Unless this is the case, an air conditioning failure is likely to require back-up operation.

Interruptions to operations with little or no damage implies that all ADP tasks will be affected but that after the cause of the interuption is cleaned up normal operation can resume at the facility. An examination of the list of typical causes shows that the duration of the interruption will depend either on the time to restore the situation, as after a computer room fire, or on external factors not under the control of the ADP facility, as with civil disorder or power failure.

Major damage refers to situations where the ADP facility is no longer tenable, back-up operation is required, and repair or reconstitution of the entire ADP facility is necessary to return to normal. The ADP security planner should see that back-up recovery plans are adequate to cope with this extreme case.

In the case of major damage or total destruction, the decision to switch to back-up operations will be obvious. In the case of limited damage or interruption it may not be as clear what to do. To make the decision wisely, the ADP manager will want to know what tasks are affected, how long it is likely to take to return to normal and who to call on for more information and assistance in making repairs or otherwise restoring the situation to normal. During his analysis of such events, the ADP security planner will have gathered much of the needed information. With a little added effort, this information can be documented to assist ADP management in making its decision. The documentation should include these elements for each likely event:

- factors which can be established in advance to estimate the duration of the interruption to normal operations.

- persons or agencies who can provide information to estimate duration of the specific event more accurately.

- persons or agencies who can be called upon to restore the situation to normal.

Some examples follow of the way this information might be assembled:

AIR CONDITIONING SYSTEM FAILURE

(1) Mean time to repair:
Circulating pump—x hours
Chiller—y hours

(2) Repair time estimates:
Building Engineering—Mr. S. Smith, Ext. 345

(3) Repair coordinator:
Building Engineering—Mr. J. Jones, Ext. 567

ELECTRIC POWER FAILURE

(1) Mean time to restore service:
Building service fault—x hours
Local service failure—y hours
Area wide failure—z hours

(2) Repair time estimates:
Building Engineering—Mr. S. Smith, Ext. 345
Power Company Dispatcher—Telephone —321-7654

(3) Repair Service:
Building Electrician—Mr. J. Jones, Ext. 789
Power Company District Repair Office —Telephone—567-6543

ADP HARDWARE FAILURE

(1) Mean time to repair:
Central Processing Unit: x hours
Multiplexer Channel: y hours
Disk Storage Control: z hours

(2) Repair time estimates:
Vendor A Representative—Ext. 543
Vendor B Representative—Ext. 789

(3) Repair coordinator:
ADP Operations Manager—
Mr. W. Brown, Ext. 555

These examples are merely intended to show how the criteria might be organized. One might include a brief discussion of the factors which affect repair time, limitations on availability of service personnel at night and on weekends and alternate contacts. It is probably not necessary to include information about events which are very unlikely to cause critical delays.

8.2. Emergency Response Planning

The term **emergency response planning** is used here to refer to steps taken immediately after an emergency occurs to protect life and property and to minimize the impact of the emergency. The "Model Facility Self-Protection Plan [14] has been designed for the general requirements of the typical Federal building. The ADP security planner should review his risk analysis to identify emergency conditions which have particular implications for ADP operations, such as protection of equipment during a period of civil commotion or loss control subsequent to a fire, flood and the like. Where he finds such situations, he should develop amendments to the Facility Self-Protection Plan to meet the special needs of the ADP facility.

He may also want to consult "Management Control of Fire Emergencies" [31], which suggests useful control procedures and "Emergency Rescue Training" [8], which contains a resume of the Office of Civil Defense Rescue Training program and includes a list of rescue equipment.

Loss control can be particularly important to the ADP facility. In a number of recent fires and floods, the value of being prepared to limit damage has been amply demonstrated. By reviewing operations and the location of critical equipment and records with Section Chiefs, the ADP security planner can develop a list of measures like these:

(1) Notify on-line users of the service interruption.
(2) Terminate jobs in progress.
(3) Rewind and demount magnetic tapes; remove disk packs; clear card readers.
(4) Power down ADP hardware and cover with plastic sheeting or other waterproof covers.
(5) Put tapes, disks, card decks, run books and source documents in a safe place.
(6) Power down air conditioning equipment.

If evacuation of work areas is ordered or likely, all personnel should be instructed to:

(1) Put working papers and the like in desks or file cabinets and close them.
(2) Turn off equipment but leave room lights on.
(3) Close doors as areas are evacuated.

The loss control plan should define the steps to be taken, assign responsibilities for general and specific steps and provide any needed materials and equipment in handy locations. In some cases there will be ample time to take all measures, but in extreme emergencies life safety will dictate immediate evacuation. For this reason the loss control plan should designate one or more individuals in each ADP area who, in the event of an emergency, shall determine what can be done to protect equipment and records without endangering life, and direct ADP staff members accordingly.

In Chapter 2 measures are discussed to protect the building against the effects of fire, flooding, windstorm and similar natural disasters. The ADP security planner should review protective plans with the building manager to assure himself that any special requirements of the ADP facility will be satisfied. At the same time, he should brief the building manager of ADP plans to get his advice and to insure good coordination. It may also be possible to make use of building management personnel to assist with ADP loss control.

When emergency response planning has been completed and approved, it should be documented succinctly for easy execution, as in the example for a fire emergency shown below:

Fire Emergency Response

1. Report fire (list phone number).
2. Assess life-safety hazard.
3. Evacuate facility if necessary.
4. Initiate loss control procedures.

8.3. Back-up Operations Planning

The risk analysis will have identified the situations in which back-up operation will probably be needed to avoid costly delays in accomplishing the missions of user agencies. The next step is to develop plans for back-up operation which are economically, technically and operationally sound. Details will depend on circumstances at the ADP facility but some general guidance can be helpful in considering the alternatives.

Back-up operations may take place on-site when there is only a partial loss of capability but may require one or more off-site locations when there has been major damage or destruction. The back-up procedures may replicate normal operation or be quite different. Quite often ADP management when considering back-up will find that an exact replica of the on-site ADP system is not available for back-up, or that the time available per day is less than what is needed to complete all assigned tasks. Fro mthis one might conclude that back-up is impossible. On the contrary, there are a number of things one can do to make back-up resources available:

Postpone the less urgent tasks. The ADP security planner should tabulate the ADP tasks in descending order of urgency as identified by the risk analysis. Having estimated the time to return to normal following a disruptive event, ADP management can quickly see which tasks can be set aside. These include such things as program development, long cycle (monthly, quarterly or annual) processing and long range planning. As long as adequate catch-up time will be available after the return to normal, there should be a number of tasks which can be safely postponed.

Substitute other procedures. If one can accept increased cost or degraded service it may be possible to use other procedures. For example, one could use punched card input for a failed OCR unit. If printer capability is lost, one could carry print tapes to a back-up facility for off-line printing. It might also be possible to substitute batch processing for on-line processing temporarily. In some cases where compatible hardware is not available, it may be feasible to maintain a second software package which is functionally identical to the regular package but technicaly compatible with the off-site ADP hardware that is available for back-up use.

Modify tasks to reduce run time. To stretch available back-up resources, it might be feasible to eliminate or postpone portions of a task, such as *information-only* reports or file updates which are not time urgent. In some cases it might help to double the cycle time for a task, e.g. run a daily task every other day instead.

By considering all these possibilities for each task, the ADP security planner will be able to develop the specifications for the minimum back-up requirements (ADP hardware, resources and hours per day) necessary for adequate back-up. These specifications can be used to evaluate potential off-site facilities. Possible sites for back-up operation include: other ADP facilities of the agency, other Federal ADP facilities and commercial service bureaus. In addition to intra-agency contacts, the ADP security planner should consult with the nearest ADP Sharing Exchange to identify possible off-site facilities. The Government-wide ADP sharing program is administered by the Offiice of Automated Management Regulations of GSA [15].

To evaluate alternate back-up modes and alternate off-site facilities, the ADP security planner should consider cost factors such as:

- ADP hardware usage charges.
- Transportation of personnel and needed supplies and materials.
- Maintenance of personnel at the off-site location.
- Transportation of input and output between users and the off-site location.
- Overtime pay for regular ADP staff members and pay for temporary personnel who may be needed.

He should also remember that some of the regular ADP costs will be reduced during back-up operation, e.g., electric power, telephone charges, hardware rentals.

As these factors come into focus—identification of critical tasks, specific back-up modes and usable off-site ADP facilities—the outlines of the optimum back-up plan will begin to emerge. In general it is wise to form several back-up plans as follows: (1) a plan for back-up operation which is not expected to extend much beyond the cause of delay, which forces a shift to back-up operation, viz., a minimum duration plan which would probably include only the most time urgent ADP tasks; (2) a plan for back-up operation for as long as it takes to reconstruct the ADP facility after total destruction, or the worse case plan, (3) plans for one or more operating periods between minimum duration and worst case and (4) a plan for each major partial failure mode.

While the individual plans will be geared to different objectives they can usually be constructed from a common set of modules. It is often most effective to make a detailed plan for total destruction since this is the most demanding situation. Scaled down versions or individual elements from this plan can then be used for the less demanding situations.

Each back-up plan should cover these five basic areas:

(1) Performance specifications. This is a statement of the specific ways in which performance of each task will depart from normal, e.g., tasks postponed, changes in cycle times, schedules, etc.

(2) User instructions. Back-up operation may require that users submit input in different forms or to different locations or may otherwise call for altered procedures. These should be clearly spelled out to avoid confusion and wasted motion.

(3) Technical requirements for each ADP task. Back-up operation of an ADP task will require the availability at the off-site ADP facility of the following: current program and data files, input data, data control and operating instruction (which may differ from normal instruction), preprinted forms, carriage control tapes, etc. These requirements must be documented for each task. Procedures also need to be established to insure that the materials needed for back-up operation are maintained off-site on a current basis.

(4) Computer system specifications. One or more off-site computer systems will have been selected for back-up operation. The following information should be recorded for each system: administrative information about the terms for and cost of back-up use, the location of the system, the configuration and software operating system, schedule of availability for back-up operation, and the tentative schedule of ADP tasks to be performed on the system.

(5) Administrative information. It is probable that back-up operation will require special personnel assignments and procedures, temporary employment or reassignment of personnel, use of special messengers and other departures from normal. Details should be documented along with guidance on obtaining required approvals.

It is quite likely that back-up requirements and the vital records management program may require retention of the same records. Therefore, the two programs should be coordinated to avoid duplication of effort.

When each of the back-up plans is completed, it should include full documentation, one purpose of which is to gain management approval. It may well be that considerable duplication will exist between individual plans, but it is recommended that each plan be completely documented in order to be sure that nothing has been overlooked. An example of a possible format is given below:

I. Emergency Evaluation Criteria

Include here information which will help ADP management to decide if back-up operation is required, as described in section 8.1.

II. Back-Up Plan A—Two Day Operation

A. Notification—include here functional titles, location, telephone numbers and information to be conveyed.

1. ADP Facility Staff
2. Off-Site Location(s)
3. Supporting Agencies
   Transportation, housing temporary personnel, communications, etc.
4. User Representatives

B. Technical Plans

1. Summary description of tasks to be performed, off-site facility, operating schedule, tasks which will not be performed, etc.
2. Task A

a. Description of operation, particularly departures from normal.

b. ADP hardware configuration and daily run time requirements.

c. Program and data files, preprinted forms and other special materials, run books, etc. required and the location(s) of back-up copies.

d. ADP staff assignments and temporary personnel requirements.

e. Special instructions for users.

f. Procedures for return to normal operations.

3. Task B
   . . . etc.

In general it will be effective to use a looseleaf format. Since not everyone will need all material, it may be well to restrict each page to a single topic. The page numbering system should allow for easy insertion of additional materials.

8.4. Recovery Planning

The use of a back-up facility usually occasions both extra expense and downgraded performance. It is therefore worthwhile to give some thought to recovery and to develop and maintain supporting documents which will minimize the time required for recovery. Furthermore, the ADP staff will be hard pressed by back-up operations. If others can handle recovery, the workload on the ADP staff will be reduced during the emergency and the process will undoubtedly be carried out more effectively and economically. Recovery from total destruction will require that these tasks be completed:

- Locate and obtain possession of enough floor space to house the ADP facility with a live load capacity as required by the ADP hardware and suitably located with respect to users and ADP staff spaces.

- Perform required modifications for needed partitions, raised floor, electric power distribution, air conditioning, communications, securty, fire safety and any other special requirements.

- Procure and install ADP hardware.

- Procure needed supplies, office equipment and furniture, tape storage racks, decollators, etc.

- Verify that all needed hardware, equipment and materials are on hand and in good working order and then transfer operations from the back-up site(s) to the reconstituted ADP facility.

If the necessary documents have been prepared in advance by the ADP staff, it should be possible for all but the last task to be completed by the agency's procurement division with only minimum support from the ADP staff. The following discussion suggests techniques for planning and developing the needed documentation and maintaining a rapid recovery capability.

The first step is to develop site-selection criteria. This need not be a major effort. The following information based on the characteristics of the existing ADP facility should be tabulated:

- A list of work areas by name, e.g., computer room, tape library, input/output control, specifying the minimum and desired square feet, live load requirement, desired proximity to other work areas, number of persons assigned to the area, major hardware and special electrical or air conditioning requirements.

- General location requirements, e.g., location of users, convenient to ADP staff residences, desired proximities (e.g., public transportation facilities, communications switching centers or other special requirements) and desired separations (e.g., avoidance of hazards from fire, flooding) as described in these Guidelines.

- Procurement requirements (e.g., cost, lease terms) which would apply.

The site-selection criteria is then reviewed and approved as appropriate. It is then used by the agency's procurement division or other responsible authority to maintain a list of two or three possible sites for reconstruction of the ADP facility, and perhaps to maintain procurement documents. Thus when disaster strikes, immediate steps can be taken to obtain needed space and modify it to accept the ADP facility. Figure 20 shows a simplified PERT diagram of such a reconstruction effort.

The second step is to prepare draft procurement documents for the ADP hardware. As a rule one would expect simply to replicate the existing configuration(s) but there are two possible exceptions. The first exception arises when the hardware delivery time may be lengthy. By consulting with the procurement division and representatives of vendors, public utilities and the like, the ADP security planner will be able to estimate the time to complete each of the activities shown in figure 20. If the estimate shows that the critical path is ADP hardware procurement, the ADP systems planners may want to consider alternate configurations, particularly if the estimated time to procure the hardware is very long. This will doubtless require software modifications but may, in fact, be the preferred alternative. The other exception is when a system configuration change (an upgrade or new system) is anticipated already. If it appears that the time required for procurement of the new configuration is about the same as for the existing configuration, it may make more sense to procure the new system rather than reconstruct the existing configuration, only to switch to the new configuration shortly thereafter.

The third step is to draft the procurement documents for needed supplies and equipment. This will include such things as:

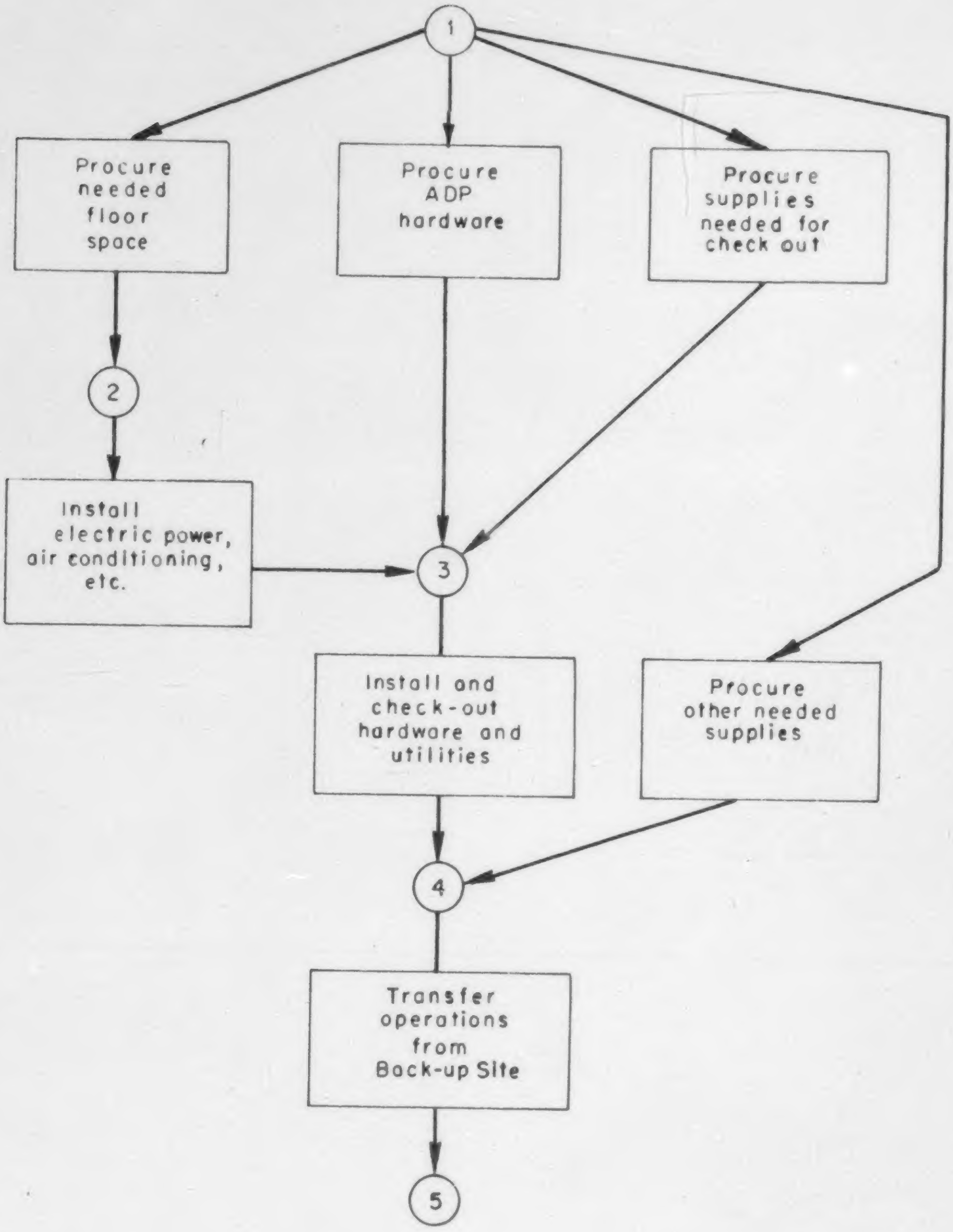

1
Procure needed floor space
Procure ADP hardware
Procure supplies needed for check out
2
Install electric power, air conditioning, etc.
3
Install and check-out hardware and utilities
Procure other needed supplies
4
Transfer operations from Back-up Site
5

FIGURE 20. *Simplified PERT diagram of ADP facility reconstruction.*

- **office furniture:** desks, chairs, tables, file cabinets, etc.
- **office machines:** typewriters, dictating equipment, adding machines, desk calculators, time clocks, duplicators, etc.
- **special ADP supplies:** magnetic tapes and disk packs, a supply of forms and punch cards, tape and disk pack storage racks, card deck storage cabinets, tape carts, decollating and bursting machines, etc.

Note that enough preprinted forms for critical tasks to last until a new supply can be procured from the vendor should be kept in a location not likely to be affected by a disaster in the ADP facility. It is not likely that the time to procure these items will constitute a critical path, but, if in doubt, the ADP security planner should check with potential sources.

The final step is to confer with the procurement division and other supporting authorities about specific regulations and any other requirements with which the ADP facility will have to comply to initiate and complete the reconstruction effort. By tabulating these regulations and the steps required to obtain procurement authority, it may be possible to identify the most time consuming steps and find ways to minimize the time required. At the same time responsibility for each reconstruction task can be assigned provisionally.

(1) Identify the critical path in the reconstruction effort and if it is unacceptably long, look for ways to reduce it.

(2) Identify the tasks which must be performed and the responsible agencies.

(3) Provide each agency with the information to proceed with its task with a minimum of help from the ADP staff during the emergency period.

8.5. Testing Contingency Plans

Since emergencies do not occur often, it will be difficult to assure adequacy and proficiency of personnel and plans without regular training and testing. Therefore, it is important to plan and budget for both. One can test for the availability of needed back-up files by attempting to repeat a particular task using on-site hardware but drawing everything else from the off-site location. Experience has demonstrated the value of such tests in validating back-up provisions; it is not uncommon to discover gross deficiences despite the most careful planning. One should verify compatibility with the off-site facility regularly by running one or more actual tasks. A number of ADP facilities conduct such tests as a part of an overall audit.

Similar tests of procedures for fire fighting, loss control, evacuation, bomb threat and other emergencies will give assurance that plans are adequate and workable and will at the same time provide an opportunity for training of ADP personnel. Each test should have a specific objective. A team should be assembled to prepare a scenario for the test, to control and observe the test, and to evaluate the results. This evaluation will provide guidance for modifications to emergency plans and for additional training. The important point is to be sure that the emergency plans have substance and do, in fact, contribute to the security of the ADP facility.

9. Security Awareness and Communications

9.0. Introduction

Throughout this handbook, many security measures have been presented, but without the dedication of the ADP staff and users in making them work, the effectiveness of a security program will be greatly diminished and some measures may not work at all. People will be more prone to feel dedicated to the security program if they understand **why there is a need** for a program, **what their involvement will be** and, particularly, **what their part is.**

In order to bring about an early awareness of the importance of the ADP security program, one should begin communicating information concerning the security program from its inception by announcing the appointment of the ADP security planner and at the same time encouraging all personnel concerned to forward their thoughts and ideas about ADP security to the planner.

As physical security measures are implemented, the general environment in the ADP facility will change. For example, access to the computer room may be curtailed. It is likely that most people will not be permitted to enter the computer room without an escort. This new security environment can have a negative psychological impact on personnel. They may feel their ability to perform their function has been limited or that their honesty and integrity has been questioned. A well developed ADP security communications program will require the support and participation of people from many organizations outside the ADP facility. Fire fighting, auditing, security, personnel, building engineering, procurement and others should participate directly. User representatives will be called upon to supply the ADP security planner with information needed to determine the loss potential due to theft of information, indirect theft of assets and delayed processing as it relates to the user's files and mission.

The objectives of the security program should be communicated to all these people as well as to the ADP staff. In particular, protection against injury or death and avoidance of episodes leading to false blame, loss of professional reputation or loss of jobs should be stressed.

9.1. Senior Management

Active involvement and participation by senior management, particularly in the chain of command above the ADP facility, is vital to developing an effective and efficient security program. Without senior management's active participation, it is doubtful that the security program will be able to reach its fullest potential. Ideally senior management's participation will involve:

- Instituting the ADP security program.
- Reviewing and approving all ADP security policy statements.
- Reviewing and approving the risk analysis and security plans.
- Determining who is responsible for documentation of the security program.
- Assisting in obtaining cooperation from those departments whose support is needed in the ADP security program, i.e., plant protection, fire safety.
- Assisting in motivating the user departments to define their data security needs.
- Budgeting the necessary funds for the ADP security program.
- Evaluating the results obtained and the performance of middle management.
- Setting a personal example of willing compliance with security rules.

9.2. Communicating the Security Program

Because of the importance of communicating the security program, a special ADP security communications plan might be developed utilizing the tools of modern communications. In developing the ADP security communications plan, the following should be considered.

9.2.1. Target Audience for the ADP Security Plan

All members of the ADP facility staff should be exposed regularly to the ADP security program. All members of organizations external to the ADP facility should receive information about the program as it may affect them.

9.2.2. Content of Communication Plan

The information presented to the ADP facility personnel should point out why it is their responsibility to protect the assets which they have under their jurisdiction and state the rules and regulations which must be followed by ADP personnel. In order for ADP personnel to better understand the security program, and, even possibly, to identify new threats or weaknesses in the existing security measures, the types of threats should be explained.

Users and personnel who support the operation of the ADP facility should be made aware of the impact a computer disaster would have upon the ability of the agency to perform its mission. It should be pointed out that if the ADP facility were damaged or destroyed, ADP tasks could not be run on time or, worse yet, vital records could be lost. In order to help user representatives to understand more clearly the information they must supply to help the ADP security planner in making the risk analysis, the impact of events such as those listed in section 1.2 should be explained to them.

9.2.3. Method of Communication

Any one or more of the following can be used to communicate the security program:

Job Descriptions. All ADP job descriptions should include a clear explanation of responsibility with regard to ADP security.

Employee Orientation. All new employees should receive an ADP security orientation lecture, either separately or as a part of the existing new employee orientation. Consideration should be given to using a form that the employee signs, stating that the employee has received the ADP security orientation and understands his specific responsibilities and the importance of ADP security to the agency. Likewise, when an employee terminates, he might be requested to sign a form stating that he will not communicate sensitive information as its relates to the secure operation of the ADP facility.

If the ADP facility is large and has many new employes, it may be worthwhile to prepare a booklet which describes the security program in general terms. It might include brief descriptions of critical area access controls, emergency procedures, the property pass system, identification cards, door key issue and other topics of general interest. If the agency already has an employee indoctrination booklet, a section on security might be added to it.

It will be appropriate to have refresher briefings on changes in the ADP security programs for all employees or at least for those in critical positions. These briefings can also be used to communicate the results of tests, drills and audits, and it should be remembered that it is just as important to report favorable results as it is to describe shortcomings.

Bulletin Board. A special security bulletin board might be installed within the ADP facility on which new security regulations are posted for ADP personnel to read and initial.

Posters. Posters are not an effective means of communicating detailed information because people have a tendency to glance at them rather than read them. But posters can reach a large audience quickly with a simple message. A number of posters on ADP security are available from the Superintendent of Documents, U.S. Government Printing Office.

News Media. If there is an employee newspaper or magazine, articles on ADP security could be published in it periodically. Pertinent articles that appear in the technical or popular press can be routed to members of the ADP staff and appropriate users.

How-to-do-it Instructions. As discussed in various other portions of this handbook, instructions should be developed for using the ADP security plan. Each individual with an assigned responsibility for security should have clear written instructions; in most cases these can be extracted from the security documentaion described in section 1.4. For example, the members of the ADP fire brigade (sec. 2.1.4) should have instructions for the actions they will take when a fire is detected.

Training. Various training tools such as films and audio cassettes, round table discussions, lectures, programmed instruction and seminars can be used for security training. A film on ADP fires is available from the National Audiovisual Center, GSA: "Fire Loss Management, Part II: Computer Installations." User groups should be oriented to the importance of ADP security, the impact that ADP security has on them and the reason why it is important that they communicate their specific requirements of the ADP security planner. Lectures and round table discussions can also be quite effective training methods since they permit face-to-face discussions and upward communication of ideas.

9.3 Summary

While it may not be easy for the ADP planner to evaluate the effectiveness and efficiency of the ADP security communications plan, the cost is modest compared with other ADP security measures. At the minimum, a communications plan is required comprising new employee orientation and a training program for ADP employees and users' groups.

When developing the ADP security program, it must be remembered that success depends on loyal and dedicated employees who comply readily with the requirements of the ADP security program. This cooperation can only be obtained if the aims and importance of the ADP security program are clearly communicated to each of them.

10. Internal Audit of Physical Security

10.0 Introduction

The previous chapters have proposed a methodology for the development of an ADP physical security program. The final element needed to complete the program is the review or audit process. The report of the NBS/ACM Workshop on Controlled Accessibility [47] defined **audit** as

"An independent and objective examination of the information system and its use (including organizational components):

a. Into the adequacy of controls, levels of risks, exposures, and compliance with standards and procedures.

b. To determine the adequacy and effectiveness of system controls versus dishonest, inefficiency, and security vulnerabilities."

The Words "independent" and "objective" are key to the definition. They imply that audit complements normal management inspections, visibility, and reporting systems, and that it is neither a part of, nor a substitute for, line management.

What can an audit be expected to accomplish? First, it evaluates security controls for the ADP facility. Second, it provides managemen an opportunity to improve and update its security program. Third, it provides the impetus to keep employees and management from becoming complacent. Last, if done effectively, it will tend to uncover areas of vulnerability. Risks change and new threats arise as systems mature.

Major factors to consider in determining the frequency of internal audits include the frequency of external audits, the rate of change of the ADP system, the amount and adequacy of controls, the threats that face the installation, and the results of previous audits. It is generally accepted that audit activity should be a matter for the highest management level which has jurisdiction over the ADP facility.

10.1. Audit Preparation

One of the main principles in audit team selection is that members should not be responsible for ADP operations. This means that the audit should be conducted by some department or agency outside of the span of control of the ADP manager. Team members should have some knowledge of data processing and, if possible, basic auditing principles. A programming or ADP operations background is desirable but not essential. An experienced user of ADP services might have the necessary qualifications. The role of the team is not to develop security controls, but to evaluate established controls and procedures. Nor should it be responsible for the enforcement of control procedures, which is clearly an ADP management responsibility.

The character of each of the audit team members is extremely important. Judgment, objectivity, ability, and a probing nature will all affect the success of the audit. The leader of the audit team must be able to organize the efforts, prepare a good written report and communicate findings effectively. If he is not technically oriented, he should be assisted by someone whose technical judgment and knowledge of ADP can be relied upon.

The size of the team depends upon the size of the installation and the scope of the audit. A large installation should consider including specialists from the following areas on the audit team:

- **Internal audit.** The knowledge and discipline to conduct an audit can be provided through internal audit specialists. Attributes of inquisitiveness, a probing nature, and attention to detail are typical characteristcs of the professional auditor. Even though the auditing profession generally is not trained in data processing technology, it should not be difficult to find an auditor with some data processing knowledge.

- **Security.** Each audit team should have some security expertise. A security officer is a welcome addition to an audit team. His role is discussed more fully in section 5.1.

- **Data processing.** Technical expertise in data processing is required. Both programming knowledge and operations experience will be helpful. Perhaps the data processing internal security officer has these skills; if so, he should be the prime candidate for the team. Using someone from the ADP facility being evaluated need not significantly affect the objectivity of the audit process.

- **Users.** Users have the most to gain from an effective audit because of their dependence on the ADP facility, yet too often they have little or no interest in ADP controls or security measures. To encourage participation in the ADP security program, one or more users who are concerned about sensitive data being compromised, disclosed, or destroyed should be encouraged to join the audit team.

- **Building management and engineering.** Many of the physical security controls to be audited—fire prevention and detection, air conditioning, electric power, access controls, and disaster prevention—relate to building management and engineering.

- **Outside specialists.** Independent, experienced viewpoints provided by outside consultants can be very helpful.

The composition of the team can be flexible. One of the prime requirements is that it consist of people who are objective. If only one ADP faciliy is to be audited, the members of the team could be assigned for the term of the audit and then returned to their normal jobs. If there are many ADP facilities under the jurisdiction of the agency, it might be advisable to establish a permanent audit team to review all installations on a recurring basis. In any event, the composition of the team should be changed periodically in order to bring in fresh viewpoints and new and different audit techniques.

10.2. The Audit Plan

In order to conduct an internal audit of security properly, a comprehensive audit plan must be developed. It should be action-oriented, listing actions to be performed. It must be tailored to the particular installation. This implies that quite a bit of work will be required in its development.

The first step is to examine the security policy for the ADP facility. This policy may apply to an entire agency, department, or a single ADP facility. In any case, it should be reviewed and pertinent security objectives extracted for subsequent investigation. The next step is to review the risk analysis plan, identifying those vulnerabilities that are significant for the particular installation. Third, the ADP Facility Security Manual, the Operations Manual and other such documents should be reviewed in order to determine what the specified security operating procedures are. And last, the ADP facility organization chart and job descriptions should be examined to identify positions with specific security or internal control responsibilities. This background material will form the basis for the development of the audit plan. There are a number of general questions that should be considered when formulating the audit program:

- What are the critical issues with regard to security? Does the ADP facility process classified or otherwise sensitive data? Does the processing duplicate that of other data centers, thereby providing some sort of back-up or contingency capability, or is it a stand-alone activity processing unique applications? What are the critical applications? What are the critical applications in terms of the audit emphasis?

- What measures are least tested in day-to-day operations? For example, if the computer fails every day at 4:15 because of power switchovers, the immediate back-up and recovery requirements are likely to be well formulated and tested. However, the complete disaster recovery plan probably will not have been tested, unless there is a specific policy to do so. This is a key point. Security measures of this type are often inadequately exercised.

- What audit activities will produce the maximum results for least effort? A test of fire detection sensors under surprise conditions will test not only the response to alarms but also the reaction of the fire brigade and the effectiveness of evacuation plans. Similarly, an attempt to get an intruder into the computer center can test not only the access control mechanisms but also the alertness of employees and security of a particular area. In interviewing personnel, questions should be designed to elicit comprehensive answers. For example, the question "How would you run an unauthorized job?" is likely to elicit more information than "Are job authorization controls effective?" The most likely answer to the second question is a simple and uninformative "Yes."

- What are the security priorities? Because of particular policy, a request for an investigation, or an incident of loss, interruption or compromise, the testing of a particular security measure probably should receive more emphasis than another equally important but non-current topic. One must, however, avoid irrational concentration on any one aspect of the program. Management over-emphasis as a result of a recent security breach should be tempered with a rational approach toward investigating all aspects of computer security.

Another step in the process of developing an audit plan is the review of previous audit reports. Many times these will identify weaknesses or concerns which should have been corrected, and so should be an item of special attention in the current audit.

Especially in the initial audit effort, one may also want to look over programs developed by other agencies if they are available, or consult publications on the subject such as the SAFE Security Audit and Field Evaluation [18] and AMR's Guide to Computer and Software Security [3]. Portions of a sample audit program adapted from the latter are shown below:

Physical Facilities

A. Fire Exposure

1. Determine that the computer is housed in a building which is fire resistant or noncombustible.
2. Determine that the computer room is separated from adjacent areas by noncombustible fire resistant partitions, walls, floors and doors and is isolated from hazardous occupancies.
3. Determine that raised floors and hung ceilings, including support hardware, are noncombustible.
4. Determine that floor coverings, furniture and window coverings are noncombustible.
5. Observe that paper and other supplies are stored outside the computer area.
6. Observe that flammable or otherwise dangerous activities are prohibited from the computer room and adjacent areas.
7. Observe that smoking is restricted in the computer area (input/output room, computer room and tape library).
8. Review training in fire fighting techniques and the assigning of individual responsibilities in case of fire.

9. Determine the adequacy and readiness of the automatic fire extinguishing systems.
10. Observe that portable fire extinguishers are placed strategically around the area with location markers clearly visible.
11. Determine that emergency power shutdown controls are easily accessible at points of exit.
12. Determine effect of emergency power shutdown.
13. Determine if a shut-down checklist is used.
14. Determine the location of smoke detectors.
15. Determine effect of activation of the smoke detection equipment. Determine that smoke detection equipment is tested on a regular basis.
16. Review the fire drill schedule and procedures.
17. Determine that an adequate supply of fire fighting water is available.
18. Review fire alarm system. Determine where the alarm is sounded.
19. Determine how the fire alarm is activated.
20. Determine the rating given to the local fire fighting force by the American Insurance Association's Standard Fire Defense Rating Schedule and review the effect of this rating on fire protection policies.
21. Inspect the supply of flammable materials used in computer maintenance. It should be in small quantities stored in approved containers.
22. Review procedure allowing emergency crews to gain access to the installation without delay.
23. Determine that a floor panel lifter is available.

B. Water Damage Exposure

1. Observe location of the computers. Are they below grade?
2. Inspect for overhead steam or water pipes. These should be for the sprinkler system only.
3. Determine if there is an adequate drainage system in the computer area, adjacent areas, and the floor above.
4. Determine if the ceiling has any holes or punctures through which water could leak.
5. Inspect electrical junction boxes under the raised flooring. They should be held off the slab to prevent water damage.
6. Determine if exterior windows and doors are watertight.
7. Determine what protection is available against accumulated rainwater or leaks in rooftop cooling towers.

C. Air Conditioning

1. Examine the air conditioning system for the computer area.
2. Determine if the duct linings and filters are noncombustible. Verify provision of fire dampers at fire rate partitions.
3. Observe the location of the compressor. It should be remote from the computer room.
4. Review the adequacy of the protection for the cooling tower.
5. Discuss the air conditioning back-up capability.
6. Examine the air intakes. They should be covered with protective screening, located above street level, and located so as to prevent intake of pollutants or other debris.
7. Examine methods for smoke removal.

D. Electricity

1. Review the monitoring of line voltage. Is a recording volt-meter used which will display transients?
2. Determine if uninterruptible and alternate power sources have been investigated.
3. Review emergency lighting system and determine source of power and how it is activated.
4. Determine if maintenance of electric power equipment is adequate.

E. Natural Disaster Exposure

1. Determine if measures taken to protect against natural disasters are adequate.
2. Determine if the building and equipment is properly grounded for lightning protection.

F. Access Control

1. Determine if exposure to vandalism has been evaluated.
2. Discuss history of vandalism at the installation.
3. Determine what access controls have been placed on building entrances. (24 hour and weekends.)
4. Discuss the round-the-clock watchman service for the computer area.
5. Review photo badge system used for positive identication of employees.
6. Determine which individuals are allowed to enter each of the vital areas of the data center.
7. Observe and test requirement to wear badges in the computer area.
8. Review the use of keys, cipher locks, badge readers, or other security devices controlling access.
9. Test the procedures used to challenge improperly identified visitors.

10. Review procedures for controlling visitors and tours of the computer area. Test the procedure.
11. Determine procedure used to prevent an individual from gaining access during off-shift hours without the presence of a security guard or another employee. Test the system.
12. Discuss agency policy concerning publicity of computer room location.
13. If access is via an electrically controlled system, determine if it can be operated by standby battery power or overridden by an accessible key.

G. Housekeeping

1. Determine method used to prevent accumulation of trash in the computer area.
2. Review schedule for cleaning equipment covers and work surfaces.
3. Determine who is responsible for washing floors. Review the schedule with them.
4. Review procedure for cleaning under raised floors. Examine the area.
5. Determine where wastebaskets are dumped. To reduce dust discharge, this should be done outside the computer area.
6. Examining carpeting and floor wax; they should be anti-static.
7. Discuss policy on eating in the computer room.
8. Determine whether or not low fire hazard waste containers are used. Observe for proper use.
9. Discuss smoking in the computer room.
10. Determine by observation that the maintenance areas are kept clean and orderly.

H. Other Facilities Considerations

1. Determine that security and operations personnel have been briefed on how to react to civil disturbances.
2. Determine that personnel know how to handle telephoned bomb threats.
3. Review and evaluate liaison program with local law enforcement agencies.

Organization and Personnel

A. Organization

1. Review organization chart and related job responsibilities.
2. Determine that critical functions are separated.
3. Discuss computer security with department management.
4. Determine who is responsible for managing computer security activities.
5. Review policy for computer security.
6. Evaluate the relationship between computer center and in-house service departments, local agencies, or outside consultants in each of the following areas:
    a. Plant engineering and facilities, construction, electrical air conditioning and site preparation.
    b. Plant or building security (fire protection, watchman, courier services, and government requirements).
    c. Vital records management.
    d. Legal staff.
    e. Personnel.
    f. Auditor (system design, policy and procedures).

B. Personnel

1. Determine policy on performing background checks of new employees for sensitive positions.
2. Determine policy on rechecking employees periodically.
3. Review cross-training of employees. Determine whether all jobs have adequate back-up.
4. Discuss the problems of disgruntled employees. Determine how management is informed and what procedures are followed.
5. Review and evaluate policies for containment or immediate dismissal of employees who may constitute a threat to the installation.
6. Determine that the department has a continuing personnel education program in computer security.

Back-Up and Recovery

A. Data and Program Back-Up

1. Determine where critical duplicate files are stored.
2. Review procedures for identifying critical files and their retention periods.
3. Review the current inventory of critical files.
4. Determine that programs are stored in low fire hazard containers.
5. Test the ease and accuracy of the file back-up system by performing a dry run. Determine if the department holds a dry run periodically.
6. Determine how back-up files are created.
7. Review write-ups of back-up and recovery procedures.

B. Back-Up Facilities

1. Review plans for a back-up computer. Determine where the installation is located, contractual agreements in effect, periodic testing, and working relationships.
2. Evaluate implementation plan for back-up installation. This plan should be reviewed and tested periodically.
3. Determine that spare parts are available locally.
4. Evaluate physical security of data files and other sensitive material stored at the back-up facility.
5. Evaluate provisions for security during emergency operation at the back-up facility.

C. Written Contingency Plan

1. Evaluate written plan determining that all significant items are covered.
2. Determine who is responsible for each functional area covered by the plan.
3. Review and evaluate the detailed notification procedure for implementation of the plan.
4. Review criteria for determining extent of disruption.
5. Determine responsibility for retaining source documents and data files for each application.
6. Review contingency training programs for EDP personnel.

Magnetic Tapes and Disks

A. Accountability

1. Determine that the tape and disk accountability procedures cover frequency of use and authorized uses.
2. Determine authorization procedures for removing tapes or disks from the vault and/or computer center.
3. Determine how the location of individual tapes or disks is accounted for.

B. Housekeeping and Storage

1. Review and evaluate the filing systems for magnetic tapes and disks.
2. Review the schedule for cleaning tapes and disks.
3. Observe that tapes are kept in their containers except when used.
4. Determine how often tape containers are cleaned.
5. Determine how often tape heads are cleaned.
6. Review policy for periodic sample testing of tapes for dropouts.
7. Determine that frayed leader is removed and discarded regularly.
8. Determine that storage vaults are designed to adequately protect tapes and disk packs.
9. Determine whether magnet detectors are or should be used.
10. Determine whether adequate protection of in-transit tapes and disks is provided.
11. Review the tape and disk rehabilitation or recertification program including back-up media.

An action oriented audit plan will comprise visual inspections, as well as examination of records and emergency response tests. If it is an initial audit, it will also include interviews with persons concerned. A chart or matrix of security involvements will help to identify the appropriate individuals to be interviewed. Figure 21 shows a simplified version for two security areas. Only a rough audit plan should be prepared before these interviews, as they should contribute substantially to the final plan.

Physical Access Controls	Requirements	Development	Review	Approval	Implementation	Maintenance
ADP Security Planner	x	x				
Users of ADP Services			x			
ADP Management			x	x		
Operations		x	x		x	
Applications Programming			x			
Building Management		x	x	x	x	x
Back-Up and Recovery						
ADP Security Planner	x	x				
Users	x		x		x	x
ADP Management			x	x		
Operations			x		x	x
Applications Programming					x	x

FIGURE 21. *Security responsibilities.*

10.3 Conducting the Audit

There are advantages to be gained from using both scheduled and surprise audits. A scheduled audit should meet the general policy requirements of the particular installation and most probably would occur no less than yearly. This could be a major audit conducted by an outside agency, an internal audit (following the guidelines above), or a spot check audit to review specialized items of interest, perhaps as a result of previous audit reports of findings. The distinguishing characteristic is that it is scheduled in advance, with a resultant flurry of preparation by the data centers. It will motivate cleaning up loose ends but will limit what can really be learned from the audit. A surprise audit, on the other hand, is designed to test on a no-notice basis certain elements of security and control. It can be accomplished by the agency or an external audit team, and it can be used to test those elements best reviewed on a surprise basis, such as fire response, access control, and personnel complacency.

In conducting an audit, the first step will normally be to interview ADP personnel, although this would not be the case if any surprise tests are required. Generally, the first walk-through would include interviews with the data processing manager and appropriate personnel. Searching, rather than leading, questions should be the rule, and the best approach is to allow the interviewee to talk as freely as possible. Ask questions to put the interviewee in the position of probing for his answer. For example, "What is your biggest access control problem?" not "Do your people wear badges?" Ask how he would accomplish illegal entry or sabotage. Don't hesitate to ask the same questions of more than one person. It is interesting how varied the responses can be. The conduct of the interviewer is important. He should strive to be open in dealing with interviewees and should avoid allusions to private information and obscure references to other people or events or in any other way cultivating an air of mystery or superiority. It goes without saying that the use of good human relations techniques is essential to a successful interview. Nothing can be gained by a belligerent interviewer who antagonizes his subject. The interviewer's conduct should be firm and inquisitive but also calm, sincere and open. Any answer which appears evasive or defensive should be probed in some detail.

The taking of notes is a matter of individual preference. Some individuals take very adequate notes at listening speed. Others must devote all their attention to listening. If note taking is a problem, the interview could be conducted by two-man teams. Another alernative is to use a portable tape recorder, making certain that the subject knows in advance that the interview is being taped. If none of the above is possible, the interviewer should attempt to listen and absorb as much as possible, then record notes and impressions directly after the conclusion of the interview.

The evaluation tests can be scheduled or come as a surprise. Most security audits should include a testing of the emergency, fire, evacuation, and disaster recovery activities. Access controls should also be tested on a no-notice basis. Tests are best scheduled or conducted early in the audit rather than after everyone is alerted to the presence of the audit team. It is possible to test the adequacy of programmed controls and data authorization by submitting jobs that attempt to bypass these controls. Care must be taken not to destroy live data. However, if ADP management believes that error detection and correction controls really work, then there should be no objection to the introduction of deliberate errors to test these controls.

The audit team should convene periodically, preferably at the end of each day's activity, to review progress and to compare notes. Areas of weakness or concern should be highlighted, and additional tests or interviews scheduled to investigate further any particular areas of concern. Copies of the audit working paper should be classified, numbered, dated and organized for ease of understanding, review, and comparison.

At the completion of the audit, a written report should be prepared immediately while impressions are still fresh. As a rule the audit report should include: (1) executive summary, (2) a description of the audit—dates, locations, scope, objectives, etc., (3) a detailed report of observations made, (4) conclusions drawn from the observations, and (5) recommendations for corrective actions as appropriate. The degree of cooperation received should be noted and favorable conclusions should be given the same prominence as deficiencies. Tables, charts, and matrices of results, statistical tests and conclusions may be very helpful. In the planning phase, agreement should be reached as to how the final report is to be distributed to the ADP facility and agency management.

10.4. Follow-Up

An audit is of little use unless it is the basis for improvement, correction, and management follow-up. The responsibility for implementation of such activity would normally reside with the ADP facility manager. He must in turn assign responsibilities for corrective action. The best approach is to summarize each major deficiency on a control sheet outlining requirements, problem definition, responsibility, action taken or required, and follow-up action. In addition an indication should be made of the date that action should be completed, or if it is to continue. Some of the corrective action may require additional funds and this should be noted.

Corrective action, follow-up, and disposition of the deficiencies should follow a recurring reporting cycle to agency management. Quarterly reports are recommended for any audit control items still open.

The final step is a frank and honest evaluation of the audit itself by ADP facility management and the audit team. A group discussion should be held with the express purpose of improving future audit procedures and process. The audit plan may be amended as needed or the team composition may need to be changed. The emphasis of the audit should always be positive—one of helping ADP management to improve the security and control of the ADP facility.

Appendix A. Glossary

Access control	Procedures, physical barriers and security personnel provided to limit access to sensitive areas.
ADP security planner	An individual with responsibility for analysis and planning of security for an ADP facility.
Annunciator	An audible or visible indicator of an alarm.
Back-up	Alternate means to permit performance of the assigned mission despite major damage or destruction of an ADP facility.
Contingency plans	Plans for emergency response, back-up operations and post-disaster recovery maintained by an ADP facility as a part of its security program.
Emanation	Electromagnetic or acoustic energy radiation and conduction from computer hardware (which may permit unintended acquisition of data streams).
Fire area	All of that portion of a building contained within fire barriers.
Fire classes	A classification of fires based on the nature of the combustibles, relating directly to the efficacy of extinguishing agents: **Class A**—Fires involving ordinary combustible solids (wood, cloth, paper, rubber and many plastics). Class B—Fires involving flammable or combustible liquids and flammable gases. Class C—Fires involving energized electrical equipment. Class D—Fires involving certain combustible materials such as magnesium and sodium.
Fire-rated	A designation given to any building component indicating that it has been designed and tested to resist the effects of a fire of given intensity for a specified period of time.
Fire safety	Procedures, practices and devices intended to provide protection of life and property against fire.
Flame spread rate	The rate at which flame travels over the surface of combustible materials. Ratings are compared with red oak which is assigned a rate of 100.
Fuel loading	A representation of potential fire severity expressed in BTUs or in pounds of combustibles per square foot of floor area. The total heat release potential for all materials is equated to a number of pounds of wood, where wood is considered to have heat release potential of 8,000 BTUs per pound.
Intrusion detector	A device designed to detect an individual crossing a line or entering an area.
Loss potential	The dollar loss which could result from physical destruction of assets, loss or theft of data, fraud or delayed processing at an ADP facility.
Proximity detector	A device which initiates a signal (alarm) when a person or object comes near (the protected object).
Seismic detector	A device which senses vibration or motion and thereby senses a physical attack upon an object or structure.
Risk analysis	An analysis of threats and loss potential for an ADP facility leading to an estimate of annual loss and selection of remedial measures.
Threat analysis	An analysis of the probability of occurrences and consequences of damaging events to an ADP facility.
Vibration detector	Seismic detector.
Zone	A division of an area protected by an alarm system. A zone can have multiple sensors or detectors but usually has only a single annunciator.

Appendix B. Bibliography

[1] Baker, H. R., P. B. Leech, and C. R. Singleterry, Surface Chemical Methods of Displacing Water and/or Oils and Salvaging Flood Equipment, U.S. Naval Research Laboratory, Washington, D.C., NRL Report 5680, September 1961, 14p.

[2] Barker, B. C., Jr., Joint-Service Interior Intrusion Detection System, in Proceedings of the 1973 Carnahan Conference on Electronic Crime Countermeasures, University of Kentucky, Lexington, College of Engineering, April 1973, p. 20-27, 2 refs.

[3] Brown, W. F., M. B. Greenlee, and R. V. Jacobson, AMR's Guide to Computer and Software Security (AMR International, Inc., New York, 1971), 208p.

[4] Brown, William F. and David H. Hawkins, Remote access computing: the executive's responsibility, Journal of Systems Management, Volume 23 (May 1972), p. 12-16.

[5] Brown, William F. and David H. Hawkins, Remote access computing: the executive's responsibility, Journal of Systems Management, Volume 23 (June 1972), p. 32-35.

[6] The Canadian Institute of Chartered Accountants, Computer Control Guidelines, Toronto, Canada, 1970, 135p.

[7] Computer Fraud and Embezzlement, EDP Analyzer, 11:9 (September 1973), p. 1-14.

[8] Emergency Rescue Training, U.S. Government Printing Office, Washington, D.C., Office of Civil Defense Student Manual SM 14-1, January 1968.

[9] Federal Fire Council, Fire Protection for Essential Electronic Equipment, Recommended Practices No. 1 (Revised), Washington, D.C., July 1969.

[10] Federal Power Commission, Power Disturbance Report, Washington, D.C. (issued quarterly; special issues on power interruptions as appropriate).

[12] Geller, S. B., The Effects of Magnetic Storage Media Used in Computers, Nat. Bur. Stand. (U.S.), Tech. Note 735, 30 pages (July 1972).

[13] General Services Administration, Building Firesafety Criteria, Washington, D.C., GSA Handbook, July 1965.

[14] General Services Administration, Model Facility Self-Protection Plan, Washington, D.C., Region 3, Federal Protective Service Division, April 1973, 37p.

[15] General Services Administration, Procurement and Contracting, Government-Wide Automated Data Management Services, in Federal Property Management Regulations, Subpart 101-32.4.

[16] Helmick, C. G., Consultant's Guide to Uninterruptible Power Supply Systems (Westinghouse Electric Corporation, Buffalo, New York, May 1972), 82p.

[17] Jacobson, D. W., Automatic Sprinkler Protection for Essential Electrical and Electronic Equipment, Fire Journal 61:1 (January 1967), p. 48-53.

[18] Krauss, L. I., Security Audit and Field Evaluation (SAFE), (Firebrand Krauss and Company, Inc., East Brunswick, New Jersey, 1972), 284p.

[19] Minnesota Mining and Manufacturing Company, Magnetic Tape Erasure—How Serious is the Threat, St. Paul, Minnesota, Magnetic Products Division, January 1972.

[20] Moore, R. T. Penetration Resistance Tests of Reinforced Concrete Barriers, U.S. Department of Commerce, National Bureau of Standards, Washington, D.C., National Bureau of Standards Interim Report 73-101, December 1972, 81p.

[21] Moore, R. T., Penetration Tests on J-SIIDS Barriers, U.S. Department of Commerce, National Bureau of Standards, Washington, D.C., National Bureau of Standards Interim Report 72-223, June 1973, 84p.

[22] National Electric Reliability Council, Review of Overall Adequacy and Reliability of the North American Bulk Power Systems, Princeton, New Jersey, September 1971.

[23] National Fire Protection Association, Care and Maintenance of Sprinkler Systems 1971, Boston, Massachusetts, NFPA Standard No. 13A, 1971, 27p.

[24] National Fire Protection Association, Fire Protection Handbook, 13th Edition, Boston, Massachusetts, 1969.

[25] National Fire Protection Association, Guard Service in Fire Loss Prevention, Boston, Massachusetts, NFPA No. 601, 1968, 15p.

[26] National Fire Protection Association, Halogenated Extinguishing Agent Systems—Halon 1301, Boston, Massachusetts, NFPA Standard No. 12A, 1971, 73p.

[27] National Fire Protection Association, Industrial Fire Brigades Training Manual, Fourth Edition, Boston, Massachusetts, 1968, 148p.

[28] National Fire Protection Association, Installation of Air Conditioning and Ventilating Systems, Boston, Massachusetts, NFPA Standard No. 90A, 1973, 32p.

[29] National Fire Protection Association, Installation of Sprinkler Systems, Boston, Massachusetts, NFPA Standard No. 13, 1973, 168p.

[30] National Fire Protection Association, Life Safety Code, Boston, Massachusetts, NFPA Standard No. 101, 1973, 241p.

[31] National Fire Protection Association, Management Control of Fire Emergencies, Boston, Massachusetts, NFPA Standard No. 7, 1967, 24p.

[32] National Fire Protection Association, Private Fire Brigades, Boston, Massachusetts, NFPA No. 27, 1967, 11p.

[33] National Fire Protection Association, Protection from Exposure Fires, Boston, Massachusetts, NFPA Standard No. 80A, 1970, 20p.

[34] National Fire Protection Association, Protection of Electronic Computer—Data Processing Equipment, Boston, Massachusetts, NFPA Standard No. 75, 1972, 33p.

[35] National Fire Protection Association, Protection of Records, Boston, Massachusetts, NFPA Standard No. 232, 1970, 93p.

[36] National Fire Protection Association, Recommended Good Practice for the Maintenance and Use of Portable Fire Extinguishers, Boston, Massachusetts, NFPA No. 10A, 1973, 35p.

[37] National Fire Protection Association, Standard for the Installation of Portable Fire Extinguishers, Boston, Massachusetts, NFPA No. 10, 1973, 40p.

[38] National Fire Protection Association, Standard for the Installation of Standpipe and Hose Systems, Boston, Massachusetts, NFPA No. 14, 1973, 26p.

[39] National Fire Protection Association, Standard for the Installation, Maintenance and Use of Auxiliary Protective Signaling Systems for Fire Alarm Service, Boston, Massachusetts, NFPA Standard No. 72B, 32p.

[40] National Fire Protection Association, Standard for the Installation, Maintenance and Use of Central Station Protective Signaling Systems for Guard, Fire Alarm and Supervisory Service, NFPA No. 71, 1972, 48p.

[41] National Fire Protection Association, Standard for the Installation, Maintenance and Use of Local Projective Signaling Systems for Watchman, Fire Alarm and Supervisory Service, Boston, Massachusetts, NFPA Standard No. 72A, 1972, 38p.

[42] National Fire Protection Association, Standard for the Installation, Maintenance and Use of Proprietary Protective Signaling Systems for Watchman, Fire Alarm and Supervisory Service, Boston, Massachusetts, NFPA Standard No. 72D, 1973, 51p.

[43] National Fire Protection Association, Standard for the Installation, Maintenance and Use of Remote Station Protective Signaling Systems, Boston, Massachusetts, NFPA Standard No. 72C, 1972, 33p.

[44] Occupational Safety and Health Administration, Portable Fire Extinguishers, Washington, D.C., OSHA Regulation 29CFR—1910. 157, 1973.

[45] Post, R. S. and A. A. Kingsbury, Security Administration—An Introduction, Thomas Books, Springfield, Illinois, 1973, 351p.

[46] Reed, Susan K. and Martha M. Gray, Controlled Accessibility Bibliography, Nat. Bur. Stand. (U.S.), Tech Note 780, 11 pages (June 1973).

[47] Reed, Susan K. and Dennis K. Branstad, Editors, Controlled Accessibility Workshop Report, Nat. Bur. Stand. (U.S.), Tech. Note 827, 86 pages (May 1974).

[48] Simpson, R. H. and M. B. Lawrence, Atlantic Hurricane Frequencies Along the U.S. Coastline, U.S. Department of Commerce, National Oceanic and Atmospheric Administration, Fort Worth, Texas, Southern Region Headquarters, National Oceanic and Atmospheric Administration Technical Memorandum NWS-SR-58, June 1971.

[49] U.S. Atomic Energy Commission, Security of Automatic Data Processing Systems, Washington, D.C., U.S. Atomic Energy Commission Manual Appendix 2703, June 1973, 37. (Unclassified)

[50] U.S. Atomic Energy Commission, Standard for Fire Protection of AEC Electronic Computer/Data Processing Systems," Washington, D.C., Division of Operational Safety, WASH 1245-1, July 1973, 38p.

[51] U.S. Department of the Army, Flood-Proofing Regulations, Washington, D.C., Office of the Chief of Engineers, June 1972, 79p.

[52] U.S. Department of Defense, Security Requirements for Automatic Data Processing (ADP) Systems, Washington, D.C., Department of Defense Directive 5200.28, December 18, 1972, 17p.

[53] U.S. Department of Defense, Industrial Security Manual for Safeguarding Classified Information—DoD 5220.22M, Washington, D.C. (available through U.S. Government Printing Office, Washington, D.C.), March 1971.

[54] U.S. Water Resources Council, Flood Hazard Evaluation Guidelines for Federal Executive Agencies, Washington, D.C., May 1972.

[55] Watt, J. H. (Ed.), NFPA Handbook of the National Electric Code, McGraw-Hill Book Company, New York, 1972, 748p.

[56] Webb, B. L., R. C. Addicks, Jr. and Claude C. Lilly (compiled by), Risk Manager's Guide, The National Underwriter Company, Cincinnati, Ohio, 1973, 590p.

[57] Westinghouse Electric Corporation, Consultants Guide to Uninterruptable Power Supply Systems, Buffalo, New York, May 1972.

[58] What to Do After the Flood, McGraw-Hill, Inc., New York, January 1965, 30p.

[59] Wright, R., S. Kramer and C. Culver, Building Practices for Disaster Mitigation, Nat. Bur. Stand. (U.S.), Bldg. Sci. Ser. 46, 474 pages (February 1973).

[60] Yourdon, Edward, Reliability of Real-Time Systems. Part 1. Different Concepts of Reliability, Modern Data, 5:1 (January 1972), p. 36-40, 42.

[61] Yourdon, Edward, Reliability of Real-Time Systems, Part 2. The Causes of System Failures, Modern Data, 5:2 (February 1972), p. 50-54, 56.

[62] Yourdon, Edward, Reliability of Real-Time Systems, Part 3. The Causes of System Failures (continued), Modern Data, 5:3 (March 1972), p. 36-41.

[63] Yourdon, Edward, Reliability of Real-Time Systems. Part 4. Examples of Real-Time System Failures, Modern Data, 5:4 (April 1972), p. 52-57.

[64] Yourdon, Edward Reliability of Real-Time Systems. Part 5. Approaches to Error Recovery, Modern Data, 5:5 (May 1972), p. 38-40, 43, 46, 48-49, 52.

[65] Yourdon, Edward, Reliability of Real-Time Systems. Part 6. Approaches to Error Recovery (continued), Modern Data 5:6 (June 1972), p. 38-39, 41-46.

Appendix C

Sample Table of Contents of a Programming Procedures Manual

CONTENTS

PREFACE

TABLE OF CONTENTS

200 GENERAL INFORMATION

- 201 Objectives of Procedures Manual
    - 201-1 Introduction and Scope
    - 201-2 Distribution and Control of Procedures Manual
    - 201-3 Organization of Procedures Manual
- 202 The Procedures Program
    - 202-1 Role of Procedures
    - 202-2 Procedures Board: Function and Membership
    - 202-3 Procedures Review Board: Function and Membership
    - 202-4 Ad Hoc Committee
    - 202-5 Procedures Documentation
    - 202-6 Procedures Classification

300 PUBLISHED PROCEDURES

400 ADMINISTRATION OF PROCEDURES

- 401 Request for New or Revised Data Processing Applications
- 402 Estimating Job Costs
- 403 Project Control Number Assignment
- 404 Interface Responsibilities: User
    - 404-1 Liaison and Inquiry
- 405 Interface Responsibilities: Operations
    - 405-1 Liaison and Inquiry
    - 405-2 Job Submission

- 406 Interface Responsibilities: Analyst
    - 406-1 Liaison and Inquiry
    - 406-2 Job Submission
- 407 Interface Responsibilities: Internal Services
    - 407-1 Keypunch
- 408 Training Responsibilities

500 DOCUMENTATION PROCEDURES

- 501 Program Issuance Control (PIC) Function
- 502 Problem Reporting
    - 502-1 Program Problems
    - 502-2 System Problems
- 503 Procedures and Systems Manual Forms Completion
    - 503-0 Job Stream Flows
    - 503-1 Job Stream Documentation
    - 503-2 Job Documentation
    - 503-3 Messages and Codes
    - 503-4 Punched Output Card
    - 503-5 Tape or Disk Data Set
    - 503-6 Form/Report
    - 503-7 Carriage Tapes
    - 503-8 Record Format
- 504 Modules
    - 504-1 Module Naming Conventions
    - 504-2 Module Folders
- 505 Programs
    - 505-1 Program Naming Conventions
    - 505-2 Program Folders
- 506 Sample Forms

600 JOB CONTROL LANGUAGE (JCL) PROCEDURES

- 601 Introduction
- 602 JCL Coding Responsibility
- 603 Job Card
- 604 Execute Card
- 605 Data Definition Card
- 606 Job Delimiter Cards
  - 606-1 Color Codes
  - 606-2 Deck Identification
  - 606-3 Columns 1 and 2 Identification
- 607 JCL Conventions
- 608 Operating System
- 609 Major Subsystems
- 610 System Input Considerations
- 611 System Output Considerations
- 612 Job Accounting
  - 612-1 Job Card Accounting Parameter
  - 612-2 Usage of Account Number
  - 612-3 User Billing Practices
- 613 Default Options

700 SOFTWARE PROCEDURES

- 701 Programming Languages Standards
  - 701-1 System Generation Options
  - 701-2 Programming Restrictions
- 702 Assembler Language Standards
  - 702-1 System Generation Option Restrictions
  - 702-2 Programming Restrictions
- 703 Standard Utilities

800 OPERATIONS PROCEDURES

- 801 Acceptance Procedures
- 802 Emergency Action (Fire, Power Failure, Etc.)
- 803 Remote Job Processing
- 804 Teleprocessing Procedures
- 805 Operations Restrictions
- 806 Scheduling
  - 806-1 Priorities
  - 806-2 Job Classes

900 DATA MANAGEMENT PROCEDURES

- 901 Data Set Identification
- 902 Retention of Data Sets
- 903 Index Structure
- 904 Volume Labeling
  - 904-1 Direct Access
  - 904-2 Tape
- 905 Partitioned Data Sets
- 906 Use of Multi-Volume Data Sets
- 907 Library Maintenance
  - 907-1 New File Processing
  - 907-2 Universal Data Set Copy Procedure
  - 907-3 Confidential Data Handling
  - 907-4 Emergency Procedures
  - 907-5 Vital Records Protection
  - 907-6 Tape Access Procedure

1000 CONTROL PROCEDURES

- 1001 Data Control
  - 1001-1 Data Element Matrix
  - 1001-2 File/Program Matrix
  - 1001-3 Module/Program Matrix

1002 Quality Control

- 1002-1 Documentation Review

1003 Security Control

- 1003-1 Equipment Protection
- 1003-2 Data Protection
- 1003-3 Computer Room Access

1004 Testing

- 1004-1 Test Steps Description
- 1004-2 Dual Run Standards

1100 CODES AND SERIAL NUMBERS

9800 PUBLICATIONS CROSS REFERENCE

9900 GLOSSARY OF TERMS

Index

- Access, control of
  - audit of 78
  - critical areas 45
  - implementation of 47, 48, 49, 50
  - requirement for 12, 45
- Air conditioning
  - air handling units 34
  - audit of 78
  - failure modes of 37
  - fire safety of 38
  - outside intakes, location of 38
  - requirement for 34
  - reliability of 37
  - typical configuration for 38
- Alarm systems
  - fire 17, 54
  - intrusion 49, 54
- Audit
  - checklists 77
  - conduct of 81
  - follow-up 82
  - frequency 76
  - objective of 75
  - planning for 76
  - reports 77, 82
  - sample program 77
  - team composition 76
- Back-up plans
  - audit of 80
  - cost of 69
  - documentation 70
  - preprinted forms 73
  - off-site facility selection 62, 63
- Communications circuits
  - back-up 41
  - dial-up 41
  - failure modes of 39
  - reliability, design for 41
  - protection for 41
  - typical configuration of 40
- Computer system reliability
  - failure mode analysis of 43
  - maintenance for improved 43
  - procurement terms for 44
  - significance of 42
  - system design for 43
  - system effectiveness ratio 44
- Construction
  - fire resistance of 16
  - penetration resistance of 50
  - security features of 49
- Contingency plans
  - (also see emergency response plans, back-up plans and recovery plans)
  - audit of 80
  - task force for 65
- Data files
  - audit of procedures used 80
  - control of 59
  - physical protection of 45
  - retention of 59
  - transit protection of 63
- Doors
  - alarms 50
  - construction of frames 50
- Drainage
  - building 22
  - computer room 22
- Earthquakes
  - probability of 23, 24
  - protection against 23
- Electric power
  - audit of 78
  - back-up for 30
  - brownouts 28
  - distribution of 27
  - failure loss estimates 29
  - failure protection 29
  - lightning, effect of 28
  - on-site generation of 32
  - recording interruptions to 28
  - shut-off switch for 32
- Elevators
  - emergency power for 42
- Emanations
  - interception of 48
  - threat from 9
- Emergency response plans
  - documentation of 69
  - loss control 68
- Failure mode analysis 43
- Federal Protection Service
  - guard services from 53
  - security surveys by 47
- Fire brigade
  - organization of 20
  - training of 20
- Fire detection
  - audit of procedures for 77
  - air conditioning, control by 18
  - function of 17
  - maintenance of 18
  - products-of-combustion 18
  - response to 18
  - system design 18
- Fire exposure
  - building construction 16
  - combustibles, amount of 16
  - occupancy 16
- Fire extinguishers
  - automatic sprinklers 19
  - carbon dioxide 19
  - halogenated agent 19
  - maintenance of 20
  - portable 18
- Fire safety
  - audit of 77
  - building operation 17
  - factors affecting 17
- Flood
  - audit of procedures for 78
  - exposure to 21
  - hurricane caused 21
  - information sources 21
  - internal 22
  - protection against 22
- Guard force
  - Federal Protective Officers 53
  - functions 18, 48, 53
  - post orders for 53
  - augmentation of 54
- Hurricanes 23
- Internal controls
  - data file access 59
  - documentation of 62
  - program changes for 60
  - programming 60
  - separation of duties for 55
- Intrusion detectors
  - area type 51
  - perimeter type 49
- Locks 48
- Loss control
  - disaster 68
  - fire damage 21
  - flood damage 21
  - windstorm 23
- Loss potential 9
- Magnetic media
  - (also see data files)

  audit of procedures for 80
  protection of 45
Maintenance
  ADP hardware 43
  fire detection 18
  rotary UPS 30
Message processors 41
Motor-generator sets 30, 33
National Electric Code 34, 39
Off-site ADP facilities
  on-site security for 63
  requirement for 62
  security at 64
  security analysis for 63
Organization of ADP facility 56
Personnel
  assignments 56
  audit of 79
  indoctrination 55
  screening 55
  selection 55
  supervision 55
  training 55
Physical protection
  construction for 50
  critical areas, of 50
  determining need for 45
  exterior doors for 48
  guard force for 53
  integration of 54
  perimeter 47, 49
  utilities, for 34, 41
Physical security program
  communication of 74
  documentation of 15
  implementation of 14
  objective of 8
  management support of 74
Programming
  acceptance testing 60
  control of 60
  documentation of 62
Recorders
  electric power 28
  temperature, humidity 38
Recovery plans
  audit of 80
  documentation of 71
  PERT diagram of 72
  preparation of 71
  procurement requirements 73
Remote terminals
  communications for 39
  emanations from 48
  protection of 63
Retention
  back-up files 59
  vital records 59
Risk analysis
  annual loss estimate 11
  benefits of 9
  loss potential estimate for 9
  threat analysis for 11
Teleprocessing
  off-site 62
  reliability of 39
  software for 41
Television, closed circuit
  entrance control 49
  exterior use of 47
  night use of 47
Threat analysis 11
Thunderstorms
  frequency of 28
Tornadoes 26
Total energy systems 42
Training
  fire brigade 20
  personnel 55
  security awareness 74
Transformer
  step-down 34
  voltage regulating 29
Transients, electric 27
Uninterruptible power supply
  multiple 36
  rotary 30
  solid state 30
  transfer switch for 30
Vital records
  Back-up planning for 59
Water Supply
  loss of 42
Windstorms
  hurricane damage 26
  hurricane frequency 23
  protection against effects of 26
  tornadoes 26

☆ U. S. GOVERNMENT PRINTING OFFICE : 1974 O - 557-874

NBS TECHNICAL PUBLICATIONS

BEST COPY AVAILABLE

PERIODICALS

JOURNAL OF RESEARCH reports National Bureau of Standards research and development in physics, mathematics, and chemistry. Comprehensive scientific papers give complete details of the work, including laboratory data, experimental procedures, and theoretical and mathematical analyses. Illustrated with photographs, drawings, and charts. Includes listings of other NBS papers as issued.

Published in two sections, available separately:

- **Physics and Chemistry (Section A)**

Papers of interest primarily to scientists working in these fields. This section covers a broad range of physical and chemical research, with major emphasis on standards of physical measurement, fundamental constants, and properties of matter. Issued six times a year. Annual subscription: Domestic, $17.00; Foreign, $21.25.

- **Mathematical Sciences (Section B)**

Studies and compilations designed mainly for the mathematician and theoretical physicist. Topics in mathematical statistics, theory of experiment design, numerical analysis, theoretical physics and chemistry, logical design and programming of computers and computer systems. Short numerical tables. Issued quarterly. Annual subscription: Domestic, $9.00; Foreign, $11.25.

DIMENSIONS/NBS (formerly Technical News Bulletin)—This monthly magazine is published to inform scientists, engineers, businessmen, industry, teachers, students, and consumers of the latest advances in science and technology, with primary emphasis on the work at NBS.

DIMENSIONS/NBS highlights and reviews such issues as energy research, fire protection, building technology, metric conversion, pollution abatement, health and safety, and consumer product performance. In addition, **DIMENSIONS/NBS** reports the results of Bureau programs in measurement standards and techniques, properties of matter and materials, engineering standards and services, instrumentation, and automatic data processing.

Annual subscription: Domestic, $6.50; Foreign, $8.25.

NONPERIODICALS

Monographs—Major contributions to the technical literature on various subjects related to the Bureau's scientific and technical activities.

Handbooks—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications—Include proceedings of high-level national and international conferences sponsored by NBS, precision measurement and calibration volumes, NBS annual reports, and other special publications appropriate to this grouping such as wall charts and bibliographies.

Applied Mathematics Series—Mathematical tables, manuals, and studies of special interest to physicists, engineers, chemists, biologists, mathematicians, computer programmers, and others engaged in scientific and technical work.

National Standard Reference Data Series—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a world-wide program coordinated by NBS. Program under authority of National Standard Data Act (Public Law 90-396). See also Section 1.2.3.

Building Science Series—Disseminates technical information developed at the Bureau on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

Technical Notes—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NBS under the sponsorship of other government agencies.

Voluntary Product Standards—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The purpose of the standards is to establish nationally recognized requirements for products, and to provide all concerned interests with a basis for common understanding of the characteristics of the products. The National Bureau of Standards administers the Voluntary Product Standards program as a supplement to the activities of the private sector standardizing organizations.

Federal Information Processing Standards Publications (FIPS PUBS)—Publications in this series collectively constitute the Federal Information Processing Standards Register. The purpose of the Register is to serve as the official source of information in the Federal Government regarding standards issued by NBS pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations). FIPS PUBS will include approved Federal information processing standards information of general interest, and a complete index of relevant standards publications.

Consumer Information Series—Practical information, based on NBS research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.

NBS Interagency Reports—A special series of interim or final reports on work performed by NBS for outside sponsors (both government and non-government). In general, initial distribution is handled by the sponsor; public distribution is by the National Technical Information Service (Springfield, Va. 22151) in paper copy or microfiche form.

Order NBS publications (except Bibliographic Subscription Services) from: Superintendent of Documents, Government Printing Office, Washington, D.C. 20402.

BIBLIOGRAPHIC SUBSCRIPTION SERVICES

The following current-awareness and literature-survey bibliographies are issued periodically by the Bureau:

Cryogenic Data Center Current Awareness Service (Publications and Reports of Interest in Cryogenics). A literature survey issued weekly. Annual subscription: Domestic, $20.00; foreign, $25.00.

Liquefied Natural Gas. A literature survey issued quarterly. Annual subscription: $20.00.

Superconducting Devices and Materials. A literature survey issued quarterly. Annual subscription: $20.00. Send subscription orders and remittances for the preceding bibliographic services to the U.S. Department of Commerce, National Technical Information Service, Springfield, Va. 22151.

Electromagnetic Metrology Current Awareness Service (Abstracts of Selected Articles on Measurement Techniques and Standards of Electromagnetic Quantities from D-C to Millimeter-Wave Frequencies). Issued monthly. Annual subscription: $100.00 (Special rates for multi-subscriptions). Send subscription order and remittance to the Electromagnetic Metrology Information Center, Electromagnetics Division, National Bureau of Standards, Boulder, Colo. 80302.

BEST COPY AVAILABLE

UNITED STATES
GOVERNMENT PRINTING OFFICE
PUBLIC DOCUMENTS DEPARTMENT
WASHINGTON, D.C. 20402

OFFICIAL BUSINESS

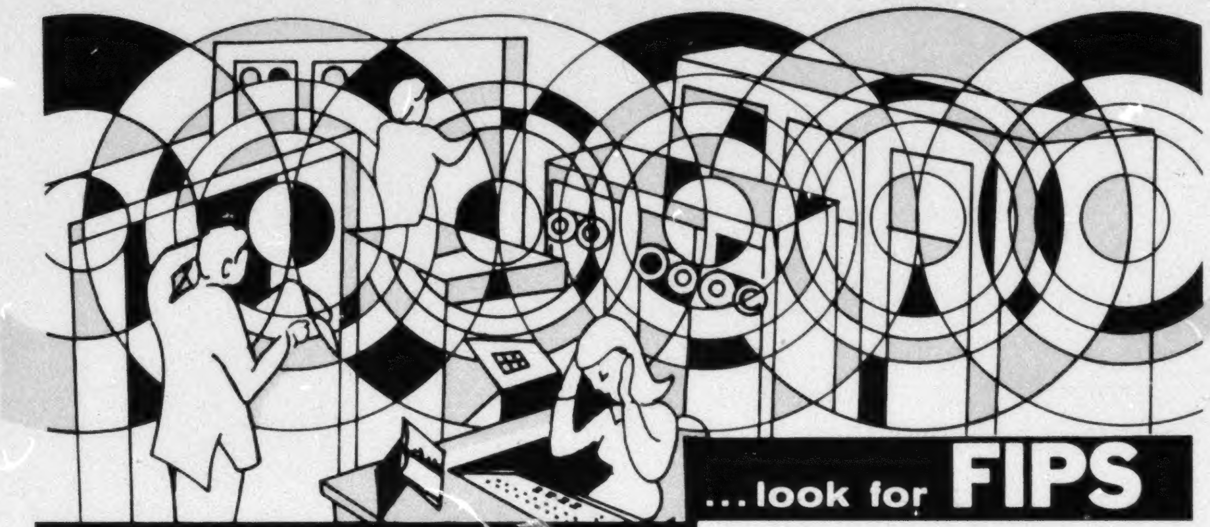
PENALTY FOR PRIVATE USE, $300

POSTAGE AND FEES PAID
U.S. GOVERNMENT PRINTING OFFICE
375

U.S.MAIL

FIPS ERICP833E R 1
ERIC PROCESSING AND
REF FACILITY STE 303
4833 RUGBY AVE
WASHINGTON DC 20014

If you're looking for a solution to your ADP standards problems . . .



DO YOU need up-to-date information on Federal Standards in the computer/information processing field?

MUST YOU keep abreast of standards adopted under PL 89-306 (Brooks Bill)?

THEN YOU need to subscribe to NBS FIPS Pub series! (Federal Information Processing Standards Publications Series of the National Bureau of Standards)

FIPS PUBS contain Federal standards for hardware, software, applications and data.
FIPS PUBS provide information on new and revised Federal standards as they become available.
FIPS PUBS are the official U.S. Government publications for Federal computer/information processing standards.
FIPS PUBS ARE AVAILABLE ON A SUBSCRIPTION BASIS FROM THE U.S. GOVERNMENT PRINTING OFFICE.

AMERICAN REVOLUTION BICENTENNIAL 1776-1976